DATENSCHUTZRECHTLICHE HERAUSFORDERUNGEN BEIM EINSATZ VON TRAININGSDATEN FÜR KI-SYSTEME

Lena Leffer / Maximilian Leicht

Wissenschaftliche Mitarbeiterin am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes, 66123 Saarbrücken, DE, lena.leffer@uni-saarland.de; legalinf.de/leffer

Wissenschaftlicher Mitarbeiter am Lehrstuhl für Rechtsinformatik sowie am Saarbrücker Zentrum für Recht und Digitalisierung (ZRD Saar) der Universität des Saarlandes, 66123 Saarbrücken, DE, maximilian.leicht@uni-saarland.de; legalinf.de/leicht

Schlagworte: ***Trainingsdaten, Künstliche Intelligenz, Maschinelles Lernen, KI-Systeme, ML-Systeme, Anonymisierung, DSGVO, Datenschutzrecht***

Abstract: *Der Beitrag setzt sich mit den datenschutzrechtlichen Problemstellungen beim Einsatz von Trainingsdaten für KI-Systeme auseinander – insbesondere mit den Anforderungen an eine Anonymisierung der Trainingsdaten und der Erforderlichkeit einer Rechtsgrundlage für eine solche Anonymisierung. Besondere datenschutzrechtliche Herausforderungen ergeben sich zudem bei der Verwendung von Bestandsdaten, die im Rahmen einer Zweckänderung verwendet werden sollen. Schließlich wird diskutiert, inwieweit die Anforderungen an die Anonymisierung dynamisch sind, das heißt die Änderung des Stands der Technik eine Anpassung der Anonymisierung erforderlich macht.*

1. Ausgangslage bei der Verwendung von Trainingsdaten

Das tägliche Leben wird mittlerweile an zahlreichen Stellen durch den Einsatz Künstlicher Intelligenz (KI) geprägt und beeinflusst.[1] Bei den dafür eingesetzten KI-Systemen handelt es sich häufig um maschinelle Lernsysteme (ML-Systeme). Diese müssen jedoch zunächst je nach ihrer Zweckbestimmung durch den Einsatz von Daten trainiert werden (sog. Trainingsdaten). Unter Trainingsdaten wird dann – im hiesigen Falle des sog. supervised learning – eine Menge an Daten verstanden, mittels derer ein Algorithmus wiederholt verschiedene Aufgabenstellung eines ähnlichen Typs lösen und mit einer vorgegebenen Lösung abgleichen kann.[2]

Unabhängig von den vielfachen vertraglichen Gestaltungsmöglichkeiten für die Verwendung und Nutzung solcher Daten stellen sich bei dem Einsatz von Trainingsdaten mit Personenbezug zahlreiche datenschutzrechtliche Fragen, die zunächst zu beantworten sind. Dieser Beitrag setzt sich mit diesen datenschutzrechtlichen Problemstellungen bei dem Einsatz von Trainingsdaten auseinander – insbesondere mit den Anforderungen an eine Anonymisierung der Trainingsdaten und der Erforderlichkeit einer Rechtsgrundlage für eine solche Anonymisierung.

2. Anonymisierung als Lösungsansatz

Die Datenschutzgrundverordnung (DSGVO) gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO. Zur Herstellung eines solchen Personenbezugs ist bereits die Identifizierbarkeit einer natürlichen Person ausreichend, Art. 4 Nr. 1 DSGVO. Hierdurch fallen auch pseudonymisierte Daten nach EG 26 Satz 2, Art. 4 Nr. 5 DSGVO ausdrücklich in den Anwendungsbereich der

[1] Tribess, in: Beck'sches Formularbuch IT-Recht, 5. Auflage 2020, 9. Datenbereitsteller-Vereinbarung (KI-Vertrag).

[2] Definition angelehnt an: Gutachten: Technische und rechtliche Betrachtungen algorithmischer Entscheidungsverfahren, S. 30, abrufbar: http://www.svr-verbraucherfragen.de/wp-content/uploads/GI_Studie_Algorithmenregulierung.pdf (zuletzt abgerufen am 05.10.2021).

DSGVO. Erst nach einer Anonymisierung der Daten sind datenschutzrechtliche Vorschriften nicht mehr anwendbar.[3] Welche exakten (rechtlichen und technischen) Anforderungen an diese Anonymisierung zu stellen sind, ist umstritten.[4]

Die gleichzeitig hohe Praxisrelevanz einer solchen Anonymisierung resultiert aus dem deutlich geringeren Ausmaß an rechtlicher Regulierung, soweit datenschutzrechtliche Vorgaben keine Anwendung finden. Zugleich muss beachtet werden, dass die Verwendung anonymer Daten zum Training von ML-Systemen auch aus technischer Perspektive gewissen Grenzen unterliegt. So ist es – je nach Anwendungsszenario des einzelnen ML-Systems – nicht immer möglich, (nur) auf anonyme Daten zurückzugreifen.[5] Zum Beispiel dürfte es beim Training einer Gesichtserkennungssoftware regelmäßig schwierig sein, lediglich anonyme Daten zu verwenden. Unter dem Stichwort „synthetische Daten" werden hierzu zwar bereits Lösungsansätze diskutiert, auch diesen begegnen aber noch rechtliche und technische Herausforderungen.[6]

Soweit dies technisch realisierbar ist, sind mit der Verarbeitung rein anonymer Daten folglich Vorteile sowohl für die verarbeitende Stelle als auch für den Schutz der Betroffenen verbunden. Dennoch sind zuvor – also bis zur vollständigen Anonymisierung der Daten – datenschutzrechtliche Anforderungen zu beachten. Auch besteht bei trainierten ML-Modellen in einigen Fällen das Risiko des Personenbezugs.[7] Im Folgenden wird daher analysiert, welche Herausforderungen bei der Anonymisierung von Trainingsdaten bestehen und welche möglichen Lösungsansätze in Betracht kommen.

3. Erforderlichkeit einer Rechtsgrundlage für die Anonymisierung der Daten

Nach EG 26 DSGVO sind Daten dann anonymisiert, wenn die Re-Identifizierbarkeit der betroffenen Person nur noch unter unverhältnismäßigem Aufwand möglich ist. Durch die Entfernung des Personenbezugs mittels des Anonymisierungsvorgangs entfällt nach Art. 2 Abs. 1 DSGVO die Anwendbarkeit des Datenschutzrechts. Denn dieses gilt nur für personenbezogene Daten.[8] Da die Daten allerdings denknotwendig zunächst einen Personenbezug aufweisen und damit in den Anwendungsbereich der DSGVO fallen, stellt sich im Vorhinein die Ausgangsfrage, ob zur Durchführung der Anonymisierung selbst eine Rechtsgrundlage erforderlich ist. Hierfür müsste zunächst eine Verarbeitung i.S.d. Art. 4 Nr. 2 DSGVO vorliegen. Nach der überwiegend vertretenen Ansicht soll bereits eine Anonymisierung der personenbezogenen Daten eine Veränderung der Daten i.S.d. Verarbeitungsbegriffes darstellen.[9] Nach dieser Ansicht wäre folglich auch der Vorgang der Anonymisierung von Daten zum Training eines ML-Modells eine Verarbeitung i.S.d. DSGVO und damit eine Rechtsgrundlage grundsätzlich erforderlich.[10] Diese Ansicht vertritt etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).[11] Ausgangspunkt der Argumentation dieser Auffassung ist die Definition des Verarbeitungsbegriffes in Art. 4 Nr. 2 DSGVO. Denn danach stellt jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezo-

---

3 Vgl. Art. 2 Abs. 1 DSGVO.

4 Winter/Battis/Halvani, Herausforderungen für die Anonymisierung von Daten, ZD 2019, 489, 489 f.

5 Vgl. Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, in: Roth/Corsten, Handbuch Digitalisierung (im Erscheinen), u.a. mit Verweis auf die exemplarische Darstellung dieser Problematik beim Einsatz von Differential Privacy: Bagdasaryan, et. al, Differential privacy has disparate impact on model accuracy, Advances in Neural Information Processing Systems 32 (2019): 15479–15488.

6 Raji, Rechtliche Bewertung synthetischer Daten für KI-Systeme, DuD 2021, 303, 304 ff.; Hittmeir et. al, On the utility of synthetic data: An empirical evaluation on machine learning tasks, Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019.

7 Vgl. Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, in: Roth/Corsten, Handbuch Digitalisierung (im Erscheinen).

8 Art. 2 Abs. 1, EG 24 S. 5 und 6 DSGVO.

9 Valkanova, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kapitel 8.1 Rn. 3.

10 Valkanova, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kapitel 8.1 Rn. 3.

11 BfDI, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche v. 29.06.2020, S. 5 (im Folgenden zitiert als: BfDI, Positionspapier Anonymisierung).

genen Daten bereits einen Verarbeitungsvorgang dar. Beispielhaft nennt die DSGVO mitunter das Erheben, Erfassen, Organisieren, Löschen und auch die Vernichtung von Daten. Bei einem weiten Begriffsverständnis wird von dem Verarbeitungsvorgang letztlich jeglicher Umgang mit personenbezogenen Daten umfasst.[12] Allein die Tatsache, dass der Personenbezug der Daten bei dem Anonymisierungsvorgang entfernt werden soll, ändert nichts an dem Verarbeitungsbegriff der DSGVO. Denn dies ist gerade die Funktion der weiten Definition in Art. 4 Nr. 2 DSGVO – es sollen alle Formen des Datenumgangs in den Anwendungsbereich des Datenschutzrechts aufgenommen werden.[13] Die Gegenansicht, die mithilfe einer genetischen Auslegung der DSGVO zu einer anderen Begriffsauslegung kommt, kann nicht überzeugen.[14] Zwar wird zurecht angeführt, dass Art. 4 Nr. 2 DSGVO die Anonymisierung nicht ausdrücklich als Beispiel einer Datenverarbeitung nennt. Allein der technische Vorgang der Anonymisierung erfordert allerdings einen Umgang mit personenbezogenen Daten, der die Voraussetzungen des Art. 4 Nr. 2 DSGVO erfüllt. Denn informationstechnisch erfolgt bei der Anonymisierung eine Aufhebung des Personenbezugs im Wege der Kürzung oder Vernichtung von Informationen.[15] Mithin stellt die Anonymisierung eine Verarbeitung i.S.d. DSGVO dar und bedarf demnach einer Rechtsgrundlage.

Zur Zulässigkeit der Durchführung der Anonymisierung müssen daher die Tatbestandsvoraussetzungen einer der in Art. 6 Abs. 1 DSGVO genannten Rechtsgrundlagen erfüllt sein.[16] Neben einer Einwilligung – sofern diese im konkreten Fall sinnvoll handhabbar ist – kommt als Rechtsgrundlage insbesondere eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO in Betracht.[17] Problematisch wird die Suche nach einer Rechtsgrundlage allerdings dann, wenn die personenbezogenen Daten besondere Kategorien personenbezogener Daten i.S.d. Art. 9 Abs. 1 DSGVO darstellen. Denn dann muss zusätzlich eine Ausnahme nach Art. 9 Abs. 2 DSGVO vorliegen.[18]

Ob einer der Ausnahmetatbestände nach Art. 9 Abs. 2 DSGVO erfüllt ist, muss im Einzelfall beurteilt werden. Grundsätzlich ist die Norm eng auszulegen – bei gleichzeitig nach dem Wortlaut sehr weitem Anwendungsbereich von Art. 9 Abs. 1 DSGVO –, sodass in vielen Fällen eine Durchführung der Anonymisierung schwierig zu rechtfertigen ist.[19] Daher werden in der Literatur verschiedene Auffassungen vertreten, warum eine Anonymisierung von besonderen Kategorien personenbezogener Daten dennoch zulässig sein soll – denn hier soll gerade ein höheres Datenschutzniveau für die betroffenen Personen erreicht werden. Damit diese Interessen der betroffenen Person und des Verantwortlichen – an dem Schutz durch (wirksame) Anonymisierung einerseits und dem Interesse an der Schaffung eines anonymisierten Datensatzes andererseits – realisiert werden können, werden schwerpunktmäßig zwei Meinungen vertreten. Die erste Auffassung geht den Weg über eine Löschungsbefugnis des Personenbezugs nach Art. 6 Abs. 1 lit. c i.V.m. Art. 17 DSGVO.[20] Dieser Auffassung folgt auch der BfDI, der Art. 17 DSGVO als rechtliche Verpflichtung zum Löschen von Daten versteht.[21] Diese Verpflichtung sei auch durch eine Anonymisierung erfüllbar[22] – insoweit kann Art. 17 DSGVO also als Rechtsgrundlage herangezogen werden. Die andere Auffassung wendet direkt oder analog Art. 6 Abs. 4 DSGVO an.[23] Vorherrschend ist in jedem Fall die Auffassung, dass ein Verbot der Anonymisierung von Daten nach Art. 9 Abs. 1 DSGVO nicht im Sinne des Unionsgesetzgebers sein kann.[24]

---

12 Thüsing/Rombey, ZD 2021, 548, 548.
13 Hornung/Wagner, ZD 2020, 223, 224.
14 Thüsing/Rombey, ZD 2021, 548, 548.
15 Hornung/Wagner, ZD 2020, 223, 224.
16 Hornung/Wagner, ZD 2020, 223, 225.
17 Hornung/Wagner, ZD 2020, 223, 225.
18 Hornung/Wagner, ZD 2020, 223, 226.
19 Hornung/Wagner, ZD 2020, 223, 226.
20 Hornung/Wagner, ZD 2020, 223, 226.
21 BfDI, Positionspapier Anonymisierung, S. 8 ff.
22 BfDI, Positionspapier Anonymisierung, S. 12; vgl. auch der Verweis auf S. 8 zur Entscheidung der österreichischen Datenschutzaufsichtsbehörde vom 5. 12.2018, Az.: DSB-D123.270/0009-DSB/2018.
23 Hornung/Wagner, ZD 2020, 223, 227.
24 Hornung/Wagner, ZD 2020, 223, 226.

4. Verwendung von Bestandsdaten als Trainingsdaten

Sofern keine anonymisierten Daten vorliegen bzw. ein Training nur mit personenbezogenen Daten durchgeführt werden kann, ist in der Praxis eine weitere Anforderung der DSGVO besonders relevant. Oft greifen Verantwortliche nämlich auf Bestandsdaten zurück, um für das Training von ML-Modellen ausreichende, qualitativ hochwertige Datenmengen verwenden zu können. Soweit bei diesen Daten ein Personenbezug vorliegt, muss der Grundsatz der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) berücksichtigt werden. Dieser sieht vor, dass personenbezogene Daten „für festgelegte, eindeutige und legitime Zwecke erhoben werden" sowie dass die Daten „nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden" (Art. 5 Abs. 1 lit. b Hs. 1 DSGVO).[25] Diese Zwecke sind den Betroffenen zum Zeitpunkt der Erhebung mitzuteilen (Art. 13 Abs. 1 lit. c DSGVO).[26]

4.1. Anforderungen an die Zweckänderung

Sollen zu einem solchen festgelegten Zweck bereits erhobene personenbezogene Daten zu einem späteren Zeitpunkt für einen anderen Zweck – etwa das Training eines ML-Modells – verarbeitet werden, sind die Vorgaben des Art. 6 Abs. 4 DSGVO zu beachten. Des Weiteren sind die Betroffenen über die beabsichtigte Weiterverarbeitung zu informieren (Art. 13 Abs. 3, Art. 14 Abs. 4 DSGVO).

Eine spätere sog. Zweckänderung kann somit grundsätzlich zulässig sein; jedoch muss der Verantwortliche feststellen, dass die Verarbeitung für den neuen Zweck mit demjenigen Zweck, zu dem die Daten ursprünglich erhoben wurden, vereinbar ist. Ob diese Vereinbarkeit gewährleistet werden kann, ist vom Verantwortlichen zu prüfen. Zumindest müssen hierfür die in Art. 6 Abs. 4 DSGVO genannten fünf Kriterien berücksichtigt werden. Die durchzuführende Prüfung wird auch als „Kompatibilitätstest" bezeichnet.[27]

Nicht erforderlich ist ein solcher Kompatibilitätstest nur in den von der Verordnung genannten Fällen. Zum einen ist dies der Fall, wenn die Verarbeitung auf einer Einwilligung der betroffenen Person beruht, Art. 6 Abs. 4 DSGVO. Dabei handelt es sich um eine deklaratorische Klarstellung: Da eine wirksame Einwilligung ohnehin stets die Anforderungen aus Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a und Art. 7 DSGVO erfüllen muss, muss sie für einen oder mehrere bestimmte Zwecke erteilt worden sein. Zwar ist es folglich grundsätzlich möglich, als Verantwortlicher eine Einwilligung für mehrere Zwecke einzuholen – pauschale Einwilligungserklärungen sind jedoch unzulässig.[28] Für im Nachhinein hinzukommende Zwecke ist die ursprüngliche Einwilligungserklärung damit untauglich. Erteilt die betroffene Person dagegen eine neue Einwilligung – in Bezug auf den geänderten Zweck der Datenverarbeitung – liegt ohnehin eine nach Art. 6 Abs. 1 DSGVO gerechtfertigte Datenverarbeitung mit eben jenem neuen Zweck vor. Insoweit stellt Art. 6 Abs. 4 DSGVO nur fest, dass in diesen Fällen ein Kompatibilitätstest entfallen kann.[29]

Zum anderen entfällt der Kompatibilitätstest, wenn die Verarbeitung „auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten [beruht], die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt" (Art. 6 Abs. 4 DSGVO). Relevant ist für nichtöffentliche Stellen dabei § 24 BDSG. Dieser adressiert etwa die Weiterverarbeitung von personenbezogenen Daten zu Zwecken der Gefahrenabwehr oder der Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche.[30]

---

25 Eine Ausnahme vom Grundsatz der Zweckbindung formuliert dagegen Art. 5 Abs. 1 lit. b Hs. 2 DSGVO in Bezug auf „Weiterverarbeitung[en] für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke."

26 Soweit die Daten nicht direkt bei der betroffenen Person erhoben wurden, vgl. Art. 14 Abs. 1 lit. c, Abs. 3 DSGVO.

27 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 186.

28 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 179.

29 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 179.

30 Weitergehende Möglichkeiten für öffentliche Stellen finden sich in § 23 BDSG.

Fällt die Verarbeitung personenbezogener Daten zum Zwecke des Trainings eines ML-Modells im Einzelfall nicht unter diese Ausnahmen – was typischerweise der Fall sein dürfte – ist der Kompatibilitätstest durchzuführen. Um eine zulässige Weiterverarbeitung zu ermöglichen, muss der Verantwortliche also feststellen, „ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist." Ist dies der Fall – ist der neue Zweck also mit dem alten Zweck der Datenverarbeitung kompatibel –, ist eine Weiterverarbeitung zulässig. Um diese Feststellung treffen zu können, muss der Verantwortliche verschiedene Kriterien berücksichtigen. Fünf davon sind explizit im Wortlaut von Art. 6 Abs. 4 DSGVO angelegt.

Besonders relevant für die Weiterverarbeitung potentieller Trainingsdaten ist das in Art. 6 Abs. 4 lit. e DSGVO angelegte Kriterium: „das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann." Pseudonymisierung ist nach dem Verständnis der DSGVO eine Verarbeitung personenbezogener Daten, nach der die Daten zwar immer noch als personenbezogen anzusehen sind (Art. 4 Nr. 5, EG 26 S. 2 DSGVO). Allerdings soll eine Zuordnung zu einer spezifischen betroffenen Person nur noch unter Hinzuziehung zusätzlicher Informationen möglich sein, welche „gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen [...]", Art. 4 Nr. 5 DSGVO. Es handelt sich damit um eine Verarbeitung personenbezogener Daten, nach welcher der Personenbezug der Daten zwar immer noch besteht, jedoch „verringert" wird. Folglich ist auch das Risiko für die Rechte und Freiheiten betroffener Personen geringer. Soweit Verantwortlichen ein Training mit pseudonymisierten Daten unter funktionalen Aspekten möglich ist, handelt es sich hierbei daher um eine datenschutzfreundliche Vorgehensweise, die im Rahmen des Kompatibilitätstests positiv zu berücksichtigen ist. Dies gilt gerade dann, wenn die Pseudonymisierung bei demselben Verantwortlichen stattfindet, die Daten also nicht an Dritte übermittelt werden, um die Pseudonymisierung durchzuführen.[31] Besondere Relevanz hat dies auch im Forschungskontext, vgl. Art. 5 Abs. 1 lit. b Hs. 2 i.V.m. Art. 89 Abs. 1 DSGVO.[32] Da Art. 6 Abs. 4 lit. e DSGVO die Maßnahmen der Verschlüsselung oder Pseudonymisierung nur exemplarisch nennt, besteht hier ein durchaus breiteres Potential für technische und organisatorische Schutzmaßnahmen, die – richtig implementiert – die Kompatibilitätsprüfung zugunsten der Weiterverarbeitung für Zwecke des Trainings von ML-Systemen beeinflussen können. Eine entsprechend transparente Dokumentation des Verantwortlichen, die mögliche Risiken sowie entsprechende Schutzmaßnahmen adressiert, dürfte in der Praxis für ein gewisses Maß an Argumentationsspielraum – auch gegenüber Datenschutzaufsichtsbehörden – sorgen.[33]

Nach Art. 6 Abs. 4 lit. d DSGVO sind zudem „die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen" zu berücksichtigen. Umfasst sind sowohl positive als auch negative Folgen für Betroffene.[34] Für das Training von ML-Systemen relevant ist diesbezüglich vor allem, dass auch hier eine Übermittlung der Daten an Dritte in Bezug auf die Kompatibilität negativ zu berücksichtigen sein soll.[35]

Daneben sind die Kriterien nach Art. 6 Abs. 4 lit. a-c DSGVO zu berücksichtigen. Nach Art. 6 Abs. 4 lit. a DSGVO ist zunächst jede Verbindung zwischen den Zwecken bei Erhebung der Daten und den Zwecken der beabsichtigten Weiterverarbeitung zu berücksichtigen. Je enger diese Verbindung ist, desto eher liegen kompatible Zwecke vor. So soll eine enge Verbindung etwa vorliegen, wenn zwischen den Zwecken ein logischer, zeitlicher Zusammenhang besteht, welcher auch für betroffene Personen naheliegend erscheint.[36] Des Weiteren ist nach Art. 6 Abs. 4 lit. b DSGVO der „Zusammenhang, in dem die personenbezogenen Daten

31 Paal/Pauly, DSGVO, 3. Aufl. 2021, Art. 6, Rn. 50.

32 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 191, 192.

33 Mögliche Risiken bestehen bspw. in sog. Model Inversion Attacks, die zunehmend auch aus rechtlicher Perspektive beleuchtet werden. Vgl. hierzu: Veale et. al, Algorithms that remember: model inversion attacks and data protection law, Philosophical Transactions of the Royal Society A, vol. 376, issue 2133; von Maltzan/Käde, Algorithmen, die nicht vergessen – Model Inversion Attacks und deren Bedeutung für den Schutz der Daten und der Urheberrechte, DSRITB 2020, 505, 505 ff.

34 Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, DSGVO, 1. Aufl. 2019, Art. 6 Abs. 4, Rn. 56; Taeger, in: Taeger/Gabel DSGVO, 3. Aufl. 2019, Art. 6, Rn. 152.

35 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 190.

36 Rossnagel, in: Simitis/Hornung/Spiecker gen. Döhmann, 1. Aufl. 2019, Art. 6, Rn. 36.

erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen“ relevant. Insbesondere in der Gesamtschau mit EG 50 DSGVO lässt sich daraus ableiten, dass die Sicht des Betroffenen ein wesentliches Merkmal der Kompatibilitätsprüfung darstellt.[37] So sieht EG 50 DSGVO vor, dass bei der Prüfung des Zusammenhangs, in welchem die Daten erhoben wurden „die vernünftigen Erwartungen der betroffenen Personen, die auf ihrer Beziehung zu dem Verantwortlichen beruhen“ mitberücksichtigt werden müssen. Schließlich ist nach Art. 6 Abs. 4 lit. c DSGVO relevant, welche Art von personenbezogenen Daten verarbeitet werden – insbesondere, ob es sich um besondere Kategorien von personenbezogenen Daten nach Art. 9 DSGVO oder um personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO handelt.

Ob die beabsichtigte Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO zulässig ist, muss folglich stets im Rahmen einer Einzelfallprüfung entschieden werden. Gerade wenn Bestandsdaten des Verantwortlichen für Zwecke des Trainings von ML-Systemen weiterverarbeitet werden sollen, sind damit stets auch gewisse Risiken verbunden – insbesondere, wenn im Rahmen einer Pseudonymisierung oder anderweitigen Datenverarbeitung eine Übermittlung der Daten an Dritte erfolgen soll. Ebenso denkbar ist eine Erhöhung des Risikos für betroffene Personen, wenn das Training der ML-Modelle – etwa mangels interner Fachkompetenz des Verantwortlichen – durch einen Dienstleister durchgeführt werden soll und hierfür eine Übermittlung der Daten an Dritte stattfindet. Gleichzeitig ist mit Art. 6 Abs. 4 lit. e DSGVO die Möglichkeit der Absicherung dieser Risiken durch geeignete Garantien ausdrücklich im Wortlaut der Verordnung festgelegt. Verantwortliche sollten die mit der Weiterverarbeitung verbundenen potenziellen Risiken daher transparent aufarbeiten und durch geeignete technische und organisatorische Schutzmaßnahmen adressieren. In Verbindung mit dem stark auslegungsbedürftigen, weiten Wortlaut der in Art. 6 Abs. 4 DSGVO genannten Kriterien ermöglicht dies einen gewissen Argumentationsspielraum, welcher von Verantwortlichen genutzt werden kann und sollte. Zugleich ist dies nicht als Freizeichnung von der Kompatibilitätsprüfung zu sehen: Grundbedingung der hier vertretenen Auffassung ist eine angemessene Adressierung der Risiken für die Rechte und Freiheiten betroffener Personen in Form der in Art. 6 Abs. 4 lit. e DSGVO genannten „geeigneten Garantien.“

4.2. Weitere Anforderungen

Eine andere Fragestellung ist, mit welchem (neuen) Zweck der alte Zweck überhaupt kompatibel sein muss, wenn das Ziel der Weiterverarbeitung die Anonymisierung der Daten ist. Hinzuweisen ist an dieser Stelle auf den sachlichen Anwendungsbereich der DSGVO – die Verordnung gilt nur für die Verarbeitung personenbezogener Daten, Art. 2 Abs. 1 DSGVO. Daraus kann abgeleitet werden, dass der neue Zweck die Anonymisierung selbst sein müsste.[38] Die hierzu erforderlichen Datenverarbeitungen wären dann zu rechtfertigen (vgl. Abschnitt 3.); überprüft werden müsste somit, ob die Anonymisierung der Daten mit dem vorherigen Zweck kompatibel ist. Anders formuliert dies der BfDI in seinem Positionspapier zur Anonymisierung unter der DSGVO: der datenschutzrechtlich relevante Zweck der Anonymisierung sei nicht die Aufhebung des Personenbezugs, „sondern das dahinterstehende tatsächliche Interesse des Verantwortlichen“[39]; der BfDI stellt insoweit also auf den Zweck ab, den der Verantwortliche in Bezug auf die Verarbeitung der (dann) anonymisierten Daten verfolgt. Kritisiert wird daran, dass das Datenschutzrecht diese Verwendung anonymisierter Daten gerade nicht reguliert; insoweit könnten die dahingehenden Interessen des Verantwortlichen nicht relevant sein.[40] Außerdem wird kritisiert, dass Art. 6 Abs. 4 DSGVO seinem Zweck nach davon ausgehe, dass nach der Weiterverarbeitung weiterhin ein Personenbezug vorliege.[41] Die Norm schränke Zweckänderungen

[37] Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6 Abs. 4, Rn. 188.
[38] Stürmer, ZD 2020, 626, 630.
[39] BfDI, Positionspapier Anonymisierung, S. 6 f.
[40] Stürmer, ZD 2020, 626, 630.
[41] Hornung/Wagner, ZD 2020, 223, 226 f.

ein, um das Risiko für Betroffene bei der Verarbeitung eben jener weiterhin personenbezogener Daten zu minimieren. Solche Risiken würden typischerweise jedoch nicht mehr bestehen, wenn der Personenbezug entfällt. Bisher ist diese Fragestellung daher als umstritten einzuordnen. Doch auch wenn man der Ansicht des BfDI folgt, so ist mit einer wirksamen Anonymisierung eine deutliche Absenkung des Risikos für die Rechte und Freiheiten der betroffenen Personen verbunden. Insoweit wäre dies im Rahmen der Zweckänderung in Art. 6 Abs. 4 DSGVO positiv zu berücksichtigen.

Daneben ist im Kontext von Art. 6 Abs. 4 DSGVO die Frage der sog. doppelten Rechtfertigung weiterhin relevant.[42] Gemeint ist eine in der Literatur thematisierte Diskussion, ob bei der Weiterverarbeitung ursprünglich zu anderen Zwecken erhobener Daten nur die Anforderungen aus Art. 6 Abs. 4 DSGVO zu erfüllen sind – oder ob daneben eine (dann „zusätzliche") Rechtsgrundlage erforderlich ist. Gegen ein solches zusätzliches Erfordernis spricht der Wortlaut von EG 50 S. 2 DSGVO, der auf die Rechtsgrundlage verweist, auf welche der Verantwortliche bei der Erhebung der personenbezogenen Daten zurückgegriffen hat. Nach diesem Verständnis wäre Art. 6 Abs. 4 DSGVO selbst als (einzig erforderliche) Rechtsgrundlage einzuordnen.[43] Andere halten diesen Aspekt des EG mit Verweis auf Äußerungen des Europäischen Parlaments während des Gesetzgebungsprozesses für einen redaktionellen Fehler[44] und verweisen u.a. aufgrund der Regelungssystematik und des Wortlauts von Art. 6 Abs. 4 DSGVO auf das Erfordernis einer Rechtsgrundlage neben der Erfüllung der Voraussetzungen des Kompatibilitätstests.[45] Für diese Rechtsgrundlage kommen dann grundsätzlich verschiedene Normen in Betracht; vielversprechend dürfte häufig die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO sein.[46]

5. Zur Weiterentwicklung des Stands der Technik als Indikator für Handlungsverpflichtungen des Verantwortlichen

Greift der Verantwortliche bei der Verwendung von Trainingsdaten für ML-Systeme auf technische Maßnahmen, wie etwa die Durchführung von Pseudo- oder Anonymisierungen der Daten zurück, so ist eine stetige Beobachtung der Weiterentwicklung des Stands der Technik zumindest zu empfehlen. Inwieweit sie im konkreten Fall auch rechtlich verbindlich sein kann – oder sogar zu bestimmten Handlungsverpflichtungen führen kann – ist nicht abschließend geklärt. Im Folgenden werden mögliche Anknüpfungspunkte hierzu kurz skizziert. Hauptsächlich relevant sind hierfür die Anforderungen der DSGVO an die Identifizierbarkeit von natürlichen Personen. Für die Fragestellung, ob eine natürliche Person identifizierbar ist und welche Mittel hierzu nach allgemeinem Ermessen wahrscheinlich genutzt werden, verweist EG 26 S. 4 DSGVO auf „alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand [...], wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind." Bereits hier ist also auch ein Blick auf zukünftige Entwicklungen genannt. Konkret bedeutet dies beim Umgang mit anonymisierten oder pseudonymisierten Daten, dass der Verantwortliche den Fortschritt des Stands der Technik berücksichtigen muss, insbesondere ob etwa neue Entwicklungen der Datenschutzforschung in der Praxis handhabbare De-Anonymisierungsangriffe zur Folge haben können.

---

42 Niemann/Kevekordes, Machine Learning und Datenschutz (Teil 1). Grundsätzliche datenschutzrechtliche Zulässigkeit, CR 2020, 17, 24.

43 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6 Rn. 181; Albers/Veit, in: BeckOK DatenschutzR, 37. Edition, Stand: 01.05.2020, Art. 6, Rn. 72.

44 Schantz, Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, NJW 2016, 1841, 1844; Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 182; Albers/Veit, in: BeckOK DatenschutzR, 37. Edition, Stand: 01.05.2020, Art. 6, Rn. 72.

45 Buchner/Petri, in: Kühling/Buchner DSGVO, 3. Aufl. 2020, Art. 6, Rn. 183, 184; Albers/Veit, in: BeckOK DatenschutzR, 37. Edition, Stand: 01.05.2020, Art. 6, Rn. 75.

46 Vgl. Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, in: Roth/Corsten, Handbuch Digitalisierung (im Erscheinen) unter Verweis auf Kaulartz, in: Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kapitel 8.9, Rn. 44; sowie Skistims, Kapitel 8.2, Rn. 39.

Insoweit sehen die Datenschutzaufsichtsbehörden den Verantwortlichen in der Pflicht, die Anonymisierung nicht als einmalige, sondern vielmehr als „fortwährende Aufgabe“[47] zu erfüllen.[48] Gerade im Kontext der Verwendung von Trainingsdaten für ML-Modelle zeigen sich zudem erste Ansätze in der Literatur, dass bestimmte technische Angriffe – wie etwa sog. Model Inversion Attacks – die Einordnung von ML-Modellen als pseudonymisierte (und damit personenbezogene) Daten erforderlich machen könnte.[49] Diese Diskussion befindet sich – gerade in Bezug auf ihre (datenschutz-)rechtliche Einordnung – zwar noch in ihren Anfängen.[50] Dennoch sollte sie von Verantwortlichen bei der Verwendung von Trainingsdaten bereits mitgedacht werden, um mögliche rechtliche wie technische Lösungsansätze berücksichtigen zu können.[51]

6. Ausblick: KI-Verordnung

Die Europäische Kommission hat am 21.4.2021 einen Verordnungsentwurf zu harmonisierten Regelungen für Künstliche Intelligenz („Artificial Intelligence Act“) veröffentlicht. Basierend auf der im April 2018 vorgelegten Europäischen KI-Strategie[52] ist Ziel des Verordnungsentwurfes die Schaffung eines rechtlichen Rahmens für vertrauenswürdige KI.[53] Der Entwurf greift den risikobasierten Bewertungsgrundsatz aus dem Weißbuch für KI auf.[54] Durch den Grundsatz der Technologieneutralität soll dabei sichergestellt werden, dass durch diverse dynamische Elemente der weiteren Technikentwicklung Rechnung getragen werden kann.[55] Der Verordnungsentwurf sieht vor, dass künftig eine präventive Prüfung erfolgen muss, ob KI-Anwendungen besonders hohe Risiken für bestimmte Rechtsgüter bewirken könnten.[56] Dabei sollen vier verschiedene Risikostufen unterschieden werden, die in dem Entwurf näher differenziert werden.[57] KI mit einem inakzeptablen Risiko soll dadurch künftig von vorneherein verboten werden.[58]

Wesentliche Adressaten der zukünftigen Verordnung sollen sowohl die Anbieter von KI als auch deren Nutzer sein.[59] Unter den Begriff des Anbieters sollen dabei auch die Entwickler von KI-Systemen fallen, die diese unter eigenem Namen oder eigener Marke in Verkehr bringen oder in Betrieb nehmen.[60] Damit nimmt der Verordnungsentwurf – anders als etwa die DSGVO – bereits den Entwickler von KI-Systemen in die Pflicht.[61]

Besonders relevant für Trainingsdaten für KI-Systeme sind dabei die vorgesehen Art. 53, 54 des Verordnungsentwurfes. Diese sehen die Einführung sog. „Regulatory Sandboxes“ (Experimentierfelder) vor.[62] Solche Experimentierfelder sind kontrollierte Umgebungen für die Entwicklung und Testung von KI-Systemen. In-

47 BfDI, Positionspapier Anonymisierung, S. 4.

48 BfDI, Positionspapier Anonymisierung, S. 4; Stellungnahme 5/2014 der Art. 29-Gruppe (WP 216 v. 10.04.2014), S. 4.

49 Von Maltzan/Käde, Algorithmen, die nicht vergessen – Model Inversion Attacks und deren Bedeutung für den Schutz der Daten und der Urheberrechte, DSRITB 2020, 505, 515 f.; vgl. auch Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, in: Roth/Corsten, Handbuch Digitalisierung (im Erscheinen) unter Verweis u.a. auf Al-Rubaie et. al, Privacy-preserving machine learning: Threats and solutions, IEEE Security & Privacy 17.2 (2019): 49–58; Veale et. al, Algorithms that remember: model inversion attacks and data protection law, Philosophical Transactions of the Royal Society A, vol. 376, issue 2133.

50 Vgl. für weitere Erkenntnisse etwa: Veale et. al, Algorithms that remember: model inversion attacks and data protection law, Philosophical Transactions of the Royal Society A, vol. 376, issue 2133.

51 Vgl. hierzu auch Leicht/Sorge, Einsatz von KI-Systemen im Unternehmen: Datenschutzrechtliche Voraussetzungen und technische Lösungsansätze, in: Roth/Corsten, Handbuch Digitalisierung (im Erscheinen).

52 Künstliche Intelligenz für Europa, COM (2018), 237 final.

53 Begründung des Verordnungsentwurfes, S. 1, COM(2021)206; Ebert/Spiecker gen. Döhmann, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188, 1188.

54 Weißbuch zur künstlichen Intelligenz, COM (2020), 65 final.

55 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

56 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

57 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

58 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

59 Vgl. Art. 3 Nr. 2, 3 des Verordnungsentwurfes.

60 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

61 Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1188.

62 Vgl. dazu und zum Folgenden: Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1192.

teressant für das Training von KI-Systemen dürfte vor allem Art. 54 des Verordnungsentwurfes sein. Dieser sieht die Möglichkeit der Weiterverarbeitung zuvor rechtmäßig erhobener personenbezogener Daten zur Entwicklung bestimmter KI-Systeme im öffentlichen Interesse im KI-Reallabor vor. Faktisch handelt es sich hier wohl um eine gesetzliche Regelung zur Zweckvereinbarkeit im Sinne des Art. 6 Abs. 4 DSGVO.[63] Der Verordnungsentwurf stellt an eine solche Weiterverarbeitung allerdings hohe Voraussetzungen. Es muss ein erhebliches öffentliches Interesse gegeben sein, die Daten müssen zur Einhaltung der Verordnung notwendig und nicht durch anonymisierte oder synthetische Daten ersetzbar sein und alle personenbezogenen Daten müssen nach Abschluss des Verfahrens gelöscht werden.[64] Art. 54 des Verordnungsentwurfes wird in der Literatur bereits kritisch gesehen. Vor dem Hintergrund, dass personenbezogene Daten aus trainierten KI-Systemen häufig rekonstruierbar seien, sei diese Erlaubnis sehr kritisch zu betrachten.

7. Danksagung

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

[63] Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1192.
[64] Vgl. dazu und zum Folgenden: Ebert/Spiecker gen. Döhmann, NVwZ 2021, 1188, 1192.