



„Weggeforscht“ – der Podcast der
Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

DFN infobrief recht

10/2026

Oktober 2026



Eine Frage der Daten

Könnten synthetische Daten auch das staatliche KI-Training revolutionieren?

Digitale Souveränität per Gesetz?

Wie die EU mit dem Cloud and AI Development Act die eigene digitale Souveränität stärken will

Was ändert der KI-Omnibus?

Die finale Version des KI-Omnibusses ist in Kraft getreten

Kurzbeitrag: EU-Chatkontrolle - Totgesagte leben länger

Die europäischen Gesetzgeber wollen es Betreibern privater Messaging-Dienste jetzt doch erlauben, nach Darstellungen von Kindesmissbrauch zu suchen

Eine Frage der Daten

Könnten synthetische Daten auch das staatliche KI-Training revolutionieren?

Von Anna Maria Yang-Jacobi

Für das Training von KI-Modellen braucht es viele Daten. Hochschulen und Forschungseinrichtungen verfügen grundsätzlich über große Datenbestände, die sie für das KI-Training nutzen könnten. Die Daten beziehen sich aber oftmals noch auf eine identifizierbare Person, sodass datenschutzrechtliche Vorgaben einzuhalten sind. So bietet es sich auch beim KI-Training von Hochschulen und Forschungseinrichtungen an, auf sogenannte synthetische Daten zurückzugreifen. Diese könnten auf lange Sicht über die Hürden der Datenschutz-Grundverordnung (DSGVO) hinweghelfen. Jedoch stellen sich bei der Erstellung von synthetischen Datensätzen gleichermaßen komplexe datenschutzrechtliche Fragen.

I. Synthetische Daten als Erfolgsrezept?

Der Begriff der synthetischen Daten taucht seit einigen Jahren vor allem im Zusammenhang mit dem Training und der Entwicklung von KI-Modellen und -Systemen auf. Ihr Potenzial reicht vom Training generativer KI bis hin zu speziellen Feldern wie der medizinischen Forschung oder statistischen Marktanalysen. Bereits 2020 stellte das Bundesministerium für Bildung und Forschung¹ eine Richtlinie zur Förderung von Projekten zum Thema „Erzeugung von synthetischen Daten für Künstliche Intelligenz“ vor.² Synthetische Daten sollen vor allem helfen, die aufkommenden Probleme von fehlenden Datenmengen und fehlender Vielfalt von repräsentativen Daten zu bewältigen.

1. Synthetische Daten

Bei synthetischen Daten handelt es sich um künstlich erzeugte Daten, die die Eigenschaften von und Bezüge zwischen tatsächlich

existierenden Datensätzen nachahmen.³ Die Daten werden dabei regelmäßig aus einem vorhandenen Datensatz generiert. Im Erstellungsprozess der neuen Daten soll jeglicher Personenbezug aus dem ausgewählten Datensatz entfernt werden. Wenn dies gelingt und die Daten keinen Personenbezug mehr aufweisen, ist die DSGVO bezüglich dieser Daten nicht mehr anwendbar. Die Idee ist: Wenn KI-Modelle mit synthetischen Daten trainiert werden, können die in den Datensätzen enthaltenen Informationen genutzt werden, ohne auf die besondere Einhaltung der datenschutzrechtlichen Vorgaben Rücksicht zu nehmen. Unabhängig von den datenschutzrechtlichen Erleichterungen helfen synthetische Daten zudem, finanzielle und tatsächliche Probleme bei der Beschaffung, Sicherheit und Qualität von Daten zu lösen. So braucht es große Datenmengen mit bestimmter Datenqualität für das anfängliche Training von KI-Modellen und auch für die spezifischen Anpassungen, die bei der späteren sogenannten Feinabstimmung (engl. Fine-Tuning) eines KI-Modells erfolgen. Die künstlich erzeugten Daten können diesen Anforderungen teilweise einfacher gerecht werden und in größeren Mengen

¹ Seit 2025 das Bundesministerium für Forschung, Technologie und Raumfahrt.

² https://www.bmfr.bund.de/SharedDocs/Bekanntmachungen/DE/2020/07/3068_bekanntmachung.html (Alle Links dieses Beitrags wurden zuletzt am 24.8.2026 abgerufen).

³ Zeng et al., Proceedings of the 2025 Conference on Empirical Methods in Natural Language Processing, S. 24528; Alexiou/Gausling, ZD 2026, 126, 127.

selbst erstellt werden, als reale Daten erhoben und aufbereitet werden können.⁴ Die Qualität der synthetischen Daten lässt sich dabei z. B. über eindeutige Standards und ein systematisches Qualitätsmanagement sowie Validierungsverfahren sicherstellen, wobei die Daten speziell gekennzeichnet werden sollen.⁵

2. Technischer Ablauf

Es gibt verschiedene Möglichkeiten, um synthetische Daten zu erzeugen. Am gängigsten ist das Modell der sogenannten Generative Adversarial Networks (GAN). Eine Gruppe von Informatikern um den US-Amerikaner Ian Goodfellow stellte GAN als neues Modell des maschinellen Lernens erstmals 2014 vor.⁶ Das Modell verwendet eine Methode des unbeaufsichtigten Lernens mit Deep-Learning-Techniken, die von mehrschichtigen neuronalen Netzwerken geprägt ist. So konkurrieren beim GAN-Modell zwei tiefe neuronale Netze miteinander. Das erste Netz ist der sogenannte Generator und generiert zunächst zufällig neue Daten. Das zweite Netz, der Diskriminator, wurde selbst mit echten Datensätzen trainiert und bewertet die erstellten Daten dahingehend, ob die neuen Daten real oder generiert sind. Die Netzwerke optimieren sich dabei gegenseitig. So nutzt der Generator das Feedback des Diskriminators, um verbesserte und realistischere Daten zu erzeugen, und der Diskriminator wird gleichzeitig besser darin, echte oder gefälschte Daten zu identifizieren. Abschließend werden mithilfe des Generators realistische Daten erzeugt, die den echten Daten statistisch ähnlich sind und ähnliche Zusammenhänge aufweisen. Am Ende des Prozesses liegt so ein synthetischer Datensatz vor.

Künstlich erstellte Daten haben allerdings nicht nur Vorteile, sondern sind auch mit Risiken verbunden. Mithilfe der GAN-Methode lassen sich zudem Bilder, Videos oder Tonspuren künstlich erzeugen. So entstehen sogenannte Deepfakes, also manipulierte Medieninhalte, deren künstlicher Ursprung oftmals nicht zu erkennen ist.⁷ Aber nicht nur synthetische Medien bergen Gefahren. So können durch synthetische Daten absichtlich Verzerrungen oder Fehler in Datensätze eingespeist werden. Außerdem gibt es beispielsweise in der Meinungsforschung riskante Entwicklungen hin zum „Synthetic Sampling“,⁸ bei dem anstelle von Antworten bzw. Meinungen echter Menschen KI-generierte Meinungen eingeholt werden. Synthetische Daten verfügen über großes Potenzial, gleichzeitig ist ihr Einsatz genau zu beobachten.

II. Synthetische Daten = anonyme Daten?

Sowohl die Anonymisierung als auch die Synthetisierung beschreiben Methoden der Depersonalisierung von Daten.⁹ Synthetische Daten finden allerdings keine Erwähnung in der DSGVO. Anonyme Daten und ihre Abgrenzung zu personenbezogenen und pseudonymen Daten werden im Datenschutzrecht jedoch bereits seit der zunehmenden Digitalisierung und dem Aufkommen neuer Technologien diskutiert.¹⁰ Aus technischer Sicht ist es nicht möglich, eine vollkommene Anonymisierung zu gewährleisten.¹¹ Aus rechtlicher Sicht ist genau diese Abgrenzung jedoch entscheidend, da das europäische Datenschutzrecht lediglich personenbezogene Daten schützt (vgl. Art. 1 Abs. 1 DSGVO). Die DSGVO definiert personenbezogene Daten zwar nach Art. 4 Nr. 1 DSGVO als „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen“. Eine

4 Hauptmann, 7.2.2025, <https://www.egovernment.de/synthetische-daten-in-der-oeffentlichen-verwaltung-nutzen-a-c5b7853a57650db2e-1b4aef056425b5a/>.

5 Ibid.

6 Goodfellow et al., Generative Adversarial Nets, 10.6.2014, <https://arxiv.org/pdf/1406.2661>.

7 Zu den Gefahren von Deepfakes siehe nur https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/Deepfakes/deepfakes_node.html.

8 Schober, 19.6.2026, <https://orf.at/stories/3426472/>.

9 Wegner, in: Leupold/Wiebe/Glossner, IT-Recht, 4. Aufl. 2021, Rn. 7 f.; Ähnlich Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR, 56. Ed., Stand 1.5.2026, DS-GVO Art. 4 Rn. 27b. Teilweise wird die Synthetisierung auch als eine Methode der Anonymisierung gesehen: Letteri/Kipker, DuD 2024, 284, 285.

10 Vgl. Härting, NJW 2013, 2065, 2069.

11 Siehe nur Henning, 25.7.2019, <https://netzpolitik.org/2019/weitere-studie-belegt-luege-anonymer-daten/>.

Definition von anonymen Daten gibt die Verordnung aber nicht vor. Nur der Erwägungsgrund 26 S. 5 DSGVO weist darauf hin, dass die Grundsätze des Datenschutzes nicht für anonyme Daten gelten, und führt weitergehend aus, dass dies „Informationen seien, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“ Nachdem die Anfangsjahre nach Inkrafttreten der DSGVO von Diskussionen rund um ein relatives oder absolutes Verständnis von Personenbezug geprägt waren, entschied der Europäische Gerichtshof (EuGH) 2025 abschließend zugunsten des relativen Verständnisses.¹² So ist die Identifizierbarkeit von Daten von der jeweiligen Stelle und ihren Re-Identifizierungsmöglichkeiten abhängig. Die EU-Kommission will diese Rechtsprechung nun auch im Gesetzestext der DSGVO verankern und sieht im bisherigen Entwurf zur Digital-Omnibus-Verordnung entsprechende Anpassungen vor.¹³ In Anbetracht der immer größer werdenden Bedeutung der Datenanonymisierung veröffentlichte der Europäische Datenschutzausschuss (EDSA) im Juli 2026 zudem konkretere Leitlinien diesbezüglich.¹⁴

Synthetischen Daten wurde lange Zeit der Vorteil nachgesagt, dass das Risiko einer Re-Identifizierung durch die künstliche Erstellung eines neuen Datensatzes geringer wäre als bei einer Anonymisierung von Datensätzen.¹⁵ In einer Studie von 2022 entdeckten Forschende jedoch, dass auch bei synthetischen Daten ähnlich wie bei anonymen Daten im Allgemeinen dennoch Möglichkeiten bestünden, um den Personenbezug von Daten wiederherzustellen, und dass die Aussagekraft der Daten verringert sein könne.¹⁶ So sind auch bei synthetischen Daten Schutzmaßnahmen zu treffen und Verfahren, die „Differential Privacy“ erfüllen, zu bedenken. Einem Datensatz soll z. B. ein sogenanntes Rauschen, also eine Form von Störfaktoren,

hinzugefügt werden, um den Datensatz leicht zu verfälschen.¹⁷ Sofern die technischen Sicherheitsvorgaben eingehalten werden, haben synthetische Daten durch den höheren Informationsgehalt und den schwierigeren Re-Identifizierungsprozess dennoch ein hohes Nutzungspotenzial.

III. Erstellung von synthetischen Daten im Kontext von Hochschulen und Forschungseinrichtungen

Vor dem Training von KI-Modellen mit synthetischen Daten sind entsprechende synthetische Daten zunächst zu erstellen. In den meisten Fällen verarbeiten die verantwortlichen Stellen dafür personenbezogene Daten weiter, die sie bereits zu einem früheren Zeitpunkt erhoben haben. Gerade Hochschulen und Forschungseinrichtungen verfügen über eine Vielzahl von personenbezogenen Daten ihrer Studierenden oder Mitarbeitenden. Dies reicht von Daten aus Bewerbungsprozessen und Immatrikulationen bzw. Einstellungen bis hin zu Prüfungsleistungen und auch aus der laufenden Verwaltung. Auch Forschende an Hochschulen erheben im Rahmen ihrer Projekte weitere personenbezogene Daten. Bei Datenverarbeitungen an Hochschulen gelten die Hochschulen selbst als datenschutzrechtlich Verantwortliche i. S. d. DSGVO.¹⁸

Vorab ist bereits darauf hinzuweisen, dass sich die datenschutzrechtliche Beurteilung je nach Ausrichtung und Aufgabe bzw. Tätigkeitsbereich einer Hochschule oder Forschungseinrichtung unterscheidet. Zunächst kann neben der konkreten Datenverarbeitung auch die Rechtsform der Hochschule oder Forschungseinrichtung ausschlaggebend dafür sein, auf welche der Rechtsgrundlagen sie sich berufen kann. So können Hochschulen und Forschungseinrichtungen sowohl in öffentlicher Hand liegen und

¹² Ausführlich dazu Yang-Jacobi, Anonym oder pseudonym? Alles ist möglich, DFN-Infobrief Recht 2/2026.

¹³ Dazu auch Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

¹⁴ EDSA, 7.7.2026, https://www.edpb.europa.eu/system/files/2026-07/edpb_guidelines_202602_anonymisation_v1_en_0.pdf.

¹⁵ Schild, in: Wolff/Brink/v. Ungern-Sternberg, BeckOK DatenschutzR, 56. Ed., Stand 1.5.2026, DS-GVO Art. 4 Rn. 27b; kritisch und die geringere Re-Identifizierungsmöglichkeit infrage stellend Alexiou/Gausling, ZD 2026, 126, 128; Simits/Hornung/Spiecker gen. Döhmman, DatenschutzR, 2. Aufl. 2025, Art. 4 Nr. 5 Rn. 57.

¹⁶ Stadler/Oprisanu/Troncoso, 24.1.2022, <https://arxiv.org/pdf/2011.07018>.

¹⁷ Vgl. Alexiou/Gausling, ZD 2026, 126, 129; Raji, DuD 2021, 303, 306. Genauer zu Differential Privacy siehe Martini, in: Paal/Pauly, DS-GVO BDSG, 4. Aufl. 2026, DSGVO Art. 32 Rn. 33d.

¹⁸ Meyer, ZD 2024, 80, 82.

z. B. als Körperschaften des öffentlichen Rechts bzw. staatliche Einrichtungen ausgestaltet sein¹⁹ als auch in privater Trägerschaft beispielsweise als (gemeinnützige) GmbH, Verein oder auch Aktiengesellschaft wirken. Im Datenschutzrecht werden die Stellen entsprechend als öffentliche oder nicht öffentliche Stelle eingeordnet. Öffentliche oder nicht öffentliche Stellen können sich je nach Verarbeitungszweck und den jeweils anwendbaren Vorschriften auf bestimmte Rechtsgrundlagen innerhalb der DSGVO oder der nationalen Datenschutzgesetze stützen. Dabei kommt dem Zweck der Datenverarbeitung bei Hochschulen und Forschungseinrichtungen eine besondere Bedeutung zu. Für Datenverarbeitungen zu wissenschaftlichen Forschungszwecken sieht das Datenschutzrecht einige Privilegierungen vor. Diese gelten jedoch nicht für die Lehre oder im Rahmen der Hochschulverwaltung.

Die Verarbeitung i. S. d. Art. 4 Nr. 2 DSGVO umfasst jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang im Zusammenhang mit personenbezogenen Daten und zählt beispielhafte Handlungen auf. Dieser weit gefasste Wortlaut des Verarbeitungsbegriffs führt dazu, dass sich selbst die Anonymisierung personenbezogener Daten auf eine rechtmäßige Verarbeitungsgrundlage stützen muss.²⁰ Da auch bei der Synthetisierung der Personenbezug von Daten entfernt wird, gilt dies ebenso für diesen Vorgang.²¹ Sofern personenbezogene Daten, die bereits früher erhoben wurden, im Nachhinein synthetisiert werden sollen, müssten neben dem Erfordernis einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO bzw. bei Gesundheitsdaten oder anderen besonders sensiblen Daten nach Art. 9 Abs. 2 DSGVO zusätzlich die Voraussetzungen einer Zweckänderung nach Art. 6 Abs. 4 DSGVO erfüllt sein. Ausschlaggebend dafür ist der Zweckbindungsgrundsatz der DSGVO.

1. Der Zweckbindungsgrundsatz der DSGVO, die wissenschaftliche Forschung und öffentliche Stellen

Die DSGVO sieht in Art. 5 Abs. 1 DSGVO sechs Grundsätze für die Verarbeitung personenbezogener Daten vor. Neben der Rechtmäßigkeit, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit ist bei der Datenverarbeitung vor allem der sogenannte Zweckbindungsgrundsatz gemäß Art. 5 Abs. 1 lit. b DSGVO einzuhalten. So müssen personenbezogene Daten „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden [...]“. Der Zweckbindungsgrundsatz ist zentral für das Datenschutzrecht und bereits in Art. 8 Abs. 2 S. 1 der Charta der Grundrechte der Europäischen Union (GRCh) verankert. Allgemein ist so zunächst zu bestimmen, ob ein weiterer Verarbeitungszweck noch vom ursprünglichen Zweck der Erhebung der Daten abgedeckt ist.

Daneben gibt es einige Ausnahmen vom Zweckbindungsgrundsatz. So sind etwa wissenschaftliche Forschungszwecke nach Art. 5 Abs. 1 lit. b Hs. 2 DSGVO privilegiert. Die DSGVO fingiert dabei die Vereinbarkeit der Zwecke. Das bedeutet: Wenn verantwortliche Stellen personenbezogene Daten für wissenschaftliche Forschungszwecke weiterverarbeiten, unterstellt der europäische Gesetzgeber, dass diese Weiterverarbeitung mit den ursprünglichen Verarbeitungszwecken vereinbar ist, sofern die technischen und organisatorischen Garantien nach Art. 89 Abs. 1 DSGVO eingehalten werden.²² Diese Privilegierung gilt also auch, wenn die Synthetisierung der Daten zu wissenschaftlichen Forschungszwecken erfolgt. Im Rahmen der Synthetisierung von Daten für die Lehre oder Verwaltung liegt jedoch kein Fall von Art. 5 Abs. 1 lit. b Hs. 2 DSGVO vor.

Sodann könnte eine Zweckänderung i. S. d. Art. 6 Abs. 4 DSGVO vorliegen. Art. 6 Abs. 4 DSGVO regelt die Voraussetzungen für die Rechtmäßigkeit einer Weiterverarbeitung personenbezogener

¹⁹ So in Berlin, siehe § 2 Abs. 1 S. 1 Berliner Hochschulgesetz (BerIHG).

²⁰ Zur Diskussion siehe nur Leffer/Leicht, Datenschutzrechtliche Herausforderungen beim Einsatz von Trainingsdaten für KI-Systeme, S. 91, https://www.uni-saarland.de/fileadmin/upload/lehrstuhl/sorge/Paper-Downloads/IRIS22_Leffer-Leicht.pdf, sowie Raji, DuD 2021, 303, 307 und Alexiou/Gausling, ZD 2026, 126, 129.

²¹ Im Ergebnis ebenso Raji, DuD 2021, 303, 307.

²² Dies ist immer nach dem Einzelfall zu bestimmen. Der EDSA veröffentlichte im April 2026 neue Leitlinien zur Verarbeitung personenbezogener Daten für wissenschaftliche Forschungszwecke, die nun einer öffentlichen Konsultation ausgesetzt waren, https://www.edpb.europa.eu/public-consultations/guidelines-12026-on-processing-of-personal-data-for-scientific-research_en.

Daten zu einem anderen als dem ursprünglichen Zweck. Die zweckändernde Datenverarbeitung kann dabei zunächst auf der Einwilligung der betroffenen Person oder auf einer europäischen oder nationalen Rechtsvorschrift beruhen. Eine Einwilligung scheidet gegenüber öffentlichen Stellen aufgrund des ungleichen Machtverhältnisses zwischen staatlicher Stelle und Bürger:innen regelmäßig aus.²³ Es könnte jedoch eine nationale Rechtsvorschrift einschlägig sein. Diese nationale Rechtsvorschrift müsste jedoch eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellen. Art. 23 Abs. 1 DSGVO erlaubt es den Mitgliedstaaten und der Europäischen Union, durch Rechtsvorschriften bestimmte Pflichten und Rechte aus der DSGVO unter bestimmten Voraussetzungen zum Schutz der in der Vorschrift genannten Ziele zu beschränken. Diese Ziele umfassen bedeutsame Rechtsgüter wie die nationale und öffentliche Sicherheit oder auch den Schutz der Unabhängigkeit der Justiz.

Der deutsche Gesetzgeber hat im Bundesdatenschutzgesetz (BDSG) mit § 23 BDSG eine Privilegierung für öffentliche Stellen bei einer Weiterverarbeitung von Daten vorgesehen. Auch die Landesdatenschutzgesetze enthalten jeweils Regelungen, die § 23 BDSG ähneln.²⁴ Diese würden auch für öffentliche Hochschulen, die als öffentliche Stellen eingeordnet werden, gelten. Allerdings ist es umstritten, inwiefern § 23 BDSG und die landesrechtlichen Äquivalente dem Schutz der Ziele des Art. 23 Abs. 1 DSGVO dienen und insofern mit der DSGVO vereinbar sind.²⁵ Im Zweifel ist von diesen Vorschriften nur vorsichtig Gebrauch zu machen und stattdessen auf spezifische und hinreichend bestimmte Normen abzustellen.²⁶ Falls keine Einwilligung oder Vorschrift im Einklang mit Art. 23 Abs. 1 DSGVO vorliegt, ist der Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO durchzuführen, bei dem anhand verschiedener in Art. 6 Abs. 4 DSGVO genannter Kriterien geprüft wird, ob der Verarbeitungszweck mit dem

ursprünglichen Zweck der Datenerhebung vereinbar ist, um eine Vereinbarkeit der Zwecke festzustellen.

2. Rechtsgrundlagen für eine Weiterverarbeitung im Rahmen der Synthetisierung von Daten

Die Privilegierung der wissenschaftlichen Forschungszwecke bezieht sich jedoch nur auf den Zweckbindungsgrundsatz. So sind die verantwortlichen Stellen dadurch nicht vom Rechtmäßigkeitsgrundsatz nach Art. 5 Abs. 1 lit. a DSGVO befreit und es bedarf also auch bei einer Zweckänderung einer weiteren Rechtsgrundlage für die Datenverarbeitung.²⁷

Dabei kommt zunächst Art. 6 Abs. 1 DSGVO oder für besonders sensible personenbezogene Daten wie Gesundheitsdaten Art. 9 Abs. 2 DSGVO in Betracht. Im Forschungskontext ist grundsätzlich auch eine Einwilligung in eine Datenverarbeitung gemäß Art. 6 Abs. 1 lit. a DSGVO bzw. Art. 9 Abs. 2 lit. a DSGVO denkbar. Für öffentliche Stellen ist jedoch auch hier die Freiwilligkeit der Einwilligung regelmäßig fraglich.²⁸

Insofern sind für staatliche Hochschulen und Forschungseinrichtungen als öffentliche Stellen die Rechtsgrundlagen zur rechtmäßigen Datenverarbeitung nach Art. 6 Abs. 1 lit. c DSGVO (erforderliche Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung) oder Art. 6 Abs. 1 lit. e DSGVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) heranzuziehen, wobei Art. 6 Abs. 1 lit. e DSGVO den Regelfall darstellen wird. Beide Rechtsgrundlagen entfalten erst in Verbindung mit einer weiteren unionsrechtlichen oder nationalen Vorschrift ihre Wirkung.²⁹ Die entsprechende ergänzende Rechtsgrundlage muss zusätzlich die Voraussetzungen

23 Bei Hochschulen besteht dieses Abhängigkeitsverhältnis ebenso, siehe Magnusson Sjöberg, in: Corrales/Fenwick/Forgó, *New Technology Big Data and the Law*, 2017, 43, 58.

24 Bspw. Art. 6 BayDSG, § 15 BlnDSG, § 6 BbgDSG, § 4 BremDSGVOAG, § 7 DSAG LSA, § 9 DSG NRW, § 5 LDSG BW, § 6 NDSG.

25 Siehe nur Heckmann/Scheurer, in: Gola/Heckmann/Rost, *DSGVO BDSG*, 4. Aufl. 2026, BDSG § 23 Rn. 3.

26 Vgl. Frenzel, in: Paal/Pauly, *DS-GVO BDSG*, 4. Aufl. 2026, BDSG § 23 Rn. 13; Albers/Veit, in: BeckOK DatenschutzR, 56. Ed., Stand 1.2.2026, BDSG § 23 Rn. 11.

27 In der rechtswissenschaftlichen Literatur besteht eine Diskussion dazu, ob die Zweckänderung nach Art. 6 Abs. 4 DSGVO einer zusätzlichen Rechtsgrundlage bedarf. Die herrschende Meinung spricht sich dafür aus, Art. 6 Abs. 4 DSGVO lediglich als Kompatibilitätstest zu sehen, sodass es eine zusätzliche Rechtsgrundlage wie z. B. Art. 6 Abs. 1 DSGVO oder Art. 9 Abs. 2 DSGVO für die Datenverarbeitung braucht.

28 Bezogen auf Hochschulen siehe Magnusson Sjöberg, in: Corrales/Fenwick/Forgó, *New Technology Big Data and the Law*, 2017, 43, 58.

29 Schild, in: BeckOK DatenschutzR, 52. Ed., 1.2.2026, DSGVO Art. 6 Rn. 57.

des Art. 6 Abs. 2 und 3 DSGVO erfüllen; insbesondere muss also der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt oder für die Erfüllung der öffentlichen Aufgabe erforderlich sein. Grundsätzlich liegen Wissenschaft und Forschung aufgrund der Historie der Förderung von Forschung innerhalb der EU bereits im öffentlichen Interesse.³⁰ Einige Landeshochschulgesetze enthalten zudem explizite Rechtsgrundlagen zur Erhebung, Speicherung und Nutzung personenbezogener Daten durch Hochschulen.³¹ Diese stützen sich ebenfalls auf das öffentliche Interesse i. S. d. Art. 6 Abs. 1 lit. e DSGVO, sofern die Hochschulen im Rahmen der Datenverarbeitung ihre gesetzlich zugewiesenen Aufgaben wahrnehmen.³²

Es gibt jedoch auch spezielle Rechtsgrundlagen. Zum Beispiel kann sich eine Verarbeitung von besonders sensiblen Daten zur wissenschaftlichen Forschung auf Art. 9 Abs. 2 lit. j DSGVO i. V. m. § 27 BDSG stützen. Art. 9 Abs. 2 lit. j DSGVO ermöglicht die Verarbeitung besonderer Kategorien personenbezogener Daten für wissenschaftliche Forschungszwecke, sofern sie auf einer geeigneten Rechtsgrundlage beruht und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorgesehen sind. § 27 BDSG³³ konkretisiert diese Voraussetzungen für die wissenschaftliche Forschung im deutschen Recht. In den übrigen Fällen kann sich die Rechtsgrundlage für Datenverarbeitungen zu wissenschaftlichen Forschungszwecken an Hochschulen aus einem Zusammenspiel der Aufgabenzuweisung der Landeshochschulgesetze und der sogenannten Generalklausel der einschlägigen Landesdatenschutzgesetze (landesrechtliche Parallelvorschriften zu § 3 BDSG) ergeben.³⁴ Je nach Schwere bzw. Intensität des Grundrechtseingriffs durch die Datenverarbeitung kann die Generalklausel allerdings nicht hinreichend bestimmt sein.³⁵

Dies ist grundsätzlich im Einzelfall zu prüfen. Allgemein lässt sich feststellen, dass bei der Synthetisierung zwar eine große Menge an Daten verarbeitet wird, diese jedoch gerade den Personenbezug entfernt und so der Datenminimierung dient. Ohne die anfängliche und ursprüngliche Datenverarbeitung in Form der Synthetisierung der personenbezogenen Daten können gerade keine synthetischen Daten erstellt werden, weshalb der Vorgang einen notwendigen Schritt darstellt.

Bei der Frage der rechtmäßigen Datenverarbeitung im Rahmen der Synthetisierung von personenbezogenen Daten wird regelmäßig auch auf eine Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten nach Art. 6 Abs. 1 lit. f DSGVO hingewiesen.³⁶ Diese Rechtsgrundlage kann jedoch nur bei privaten Hochschulen und Forschungseinrichtungen herangezogen werden. Für staatliche Hochschulen und Forschungseinrichtungen ist demgegenüber Art. 6 Abs. 1 S. 2 DSGVO zu beachten. Danach gilt Art. 6 Abs. 1 lit. f DSGVO nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. Staatliche Hochschulen und Forschungseinrichtungen können daher bei der Wahrnehmung ihrer öffentlichen Aufgaben nicht auf die Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO zurückgreifen.³⁷

IV. Fazit

Die Synthetisierung von Daten ist ein spannender technischer Vorgang mit Förderungspotenzial, sofern technische Sicherheitsmaßnahmen eingehalten werden. Immerhin kann der Einsatz von synthetischen Daten beim KI-Training das Risiko von Datenschutzrechtsverstößen beim späteren Einsatz des Modells erheblich

30 Golla, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, 2019, § 23 Rn. 3, 42; Bronner/Wiedemann, ZD 2023, 77, 83.

31 Bspw. § 12 LHG BW, § 6 BerlHG, § 111 HmbHG oder § 15 SächsHSG.

32 Zu § 12 LHG BW siehe Landtag von Baden-Württemberg, Gesetzentwurf der Landesregierung, Viertes Gesetz zur Änderung hochschulrechtlicher Vorschriften, 20.10.2020, S. 70, https://www.landtag-bw.de/resource/blob/251186/a235752ed7de7cd25daeec3e98c6bb72/16_9090_D.pdf.

33 Oder landesrechtlichen Vorschriften wie bspw. § 17 BlnDSG.

34 Vgl. Bronner/Wiedemann, ZD 2023, 77, 83.

35 Petri, in: Kühling/Buchner, DS-GVO BDSG, 4. Aufl. 2024, BDSG § 3 Rn. 9.

36 Vgl. Alexiou/Gausling, ZD 2026, 126, 130 f. Bei der anders angelegten Frage des KI-Trainings mit personenbezogenen Daten wird Art. 6 Abs. 1 lit. f DSGVO auch regelmäßig als Rechtsgrundlage herangezogen, siehe dazu nur die Entscheidung des OLG Köln vorgestellt in Müller-Westphal, Ohne Widerspruch ist alles erlaubt, DFN-Infobrief Recht 10/2025.

37 Vgl. Raji, DuD 2021, 303, 309.

verringern. Auch Hochschulen und Forschungseinrichtungen verfügen über eine große Menge an personenbezogenen Daten. Somit besteht auch dort die Möglichkeit, personenbezogene Daten für sekundäre Zwecke nutzbar zu machen. Zudem ist auch bei Hochschulen und Forschungseinrichtungen das Interesse an einer effizienteren Gestaltung von Abläufen groß – gerade auch durch den Einsatz von KI. Ein Einsatz synthetischer Daten ist somit auch in diesem Bereich besonders interessant. Dabei muss jedoch gewährleistet werden, dass tatsächlich jegliche Re-Identifizierung von synthetischen Daten ausgeschlossen ist. Anderenfalls wäre die DSGVO auch bei der Verwendung synthetischer Daten je nach verantwortlicher Stelle anwendbar.

Am Ende sind synthetische Daten jedoch nur eine von vielen Möglichkeiten, die in Betracht gezogen werden müssen, um ein rechtssicheres Training von KI-Modellen auch mit personenbezogenen Daten zu ermöglichen.³⁸ Die Europäische Kommission hat im Rahmen des Gesetzgebungsverfahrens zum Vorschlag für eine Digital-Omnibus-Verordnung³⁹ unter anderem Änderungen der DSGVO angeregt, die auch die Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklung und dem Betrieb von KI-Systemen betreffen. Dabei soll klargestellt werden, dass die Verarbeitung personenbezogener Daten unter bestimmten Voraussetzungen auf ein berechtigtes Interesse i. S. d. Art. 6 Abs. 1 lit. f DSGVO gestützt werden kann (Art. 88c DSGVO-E). Weitere Erleichterungen für die Entwicklung und den Betrieb von KI-Systemen werden zudem vorgesehen. Das Gesetzgebungsverfahren zur Änderung der DSGVO ist aber noch nicht abgeschlossen. Ein konkreter Zeitpunkt für das Inkrafttreten der vorgeschlagenen Änderungen der DSGVO und damit für die mögliche Einführung eines Art. 88c DSGVO-E steht daher noch nicht fest. Für öffentliche Stellen ist zudem weiterhin gesondert zu prüfen, welche Rechtsgrundlage für die jeweilige Verarbeitung einschlägig ist. So müsste unter Umständen der nationale Gesetzgeber innerhalb der von der DSGVO vorgesehenen Grenzen tätig werden.

38 Zur urheberrechtlichen Problematik beim KI-Training siehe Leonhard, Kurzbeitrag: Minest du das im Ernst?, DFN-Infobrief Recht 5/2026 und Müller, Die Menge macht's, DFN-Infobrief Recht 11/2024.

39 Zum Vorschlag genauer Müller-Westphal, Alles bleibt anders, DFN-Infobrief Recht 2/2026.

Digitale Souveränität per Gesetz?

Wie die EU mit dem Cloud and AI Development Act die eigene digitale Souveränität stärken will

Von Dr. Paul Friedl

Der neue Cloud and AI Development Act (CADA) soll der EU helfen, zum ersten „KI-Kontinent“ der Welt zu werden. Teil des Gesetzesvorschlags ist auch ein neuer Rahmen für souveräne Cloud-Dienste. Wie viel Souveränität bringt das Gesetz und was bedeutet das Paket für Universitäten und Forschung?

I. Europas digitales Defizit

Europa hinkt in der globalen Digitalwirtschaft hinterher. Diese Diagnose ist heute unbestritten und einige ihrer Symptome lassen sich auch in Zahlen gut messen: Europa gibt im Vergleich zu seinen globalen Wettbewerbern deutlich weniger für digitale Forschung & Entwicklung aus,¹ auch Patente produziert der europäische Informationstechnologiesektor vergleichsweise wenig² und von den fünfzig wertvollsten Digitalunternehmen der Welt sind nur drei europäisch.³ Wie diesem Missstand abgeholfen werden kann, ohne andere politische Ziele aufzugeben, ist hingegen weniger offensichtlich: Teils wird vorgeschlagen, es müsse vor allem mehr privates Kapital nutzbar gemacht werden; andere wiederum sehen die aus ihrer Sicht überbordende Fülle an Regularien oder die weiter bestehende Fragmentierung des Finanzmarktes als hauptverantwortliche Auslöser. Klar ist, dass die andauernden Entwicklungsdefizite zum einen die Sicherung langfristigen Wohlstands gefährden, zum anderen aber auch zu gefährlichen technologischen Abhängigkeiten von (potenziellen) Kontrahenten führen können.⁴ Es ist vor diesem Hintergrund

wenig überraschend, dass sich die europäische Digitalstrategie neuerlich den beiden Zielen Wettbewerbsfähigkeit und digitale Souveränität verschrieben und ein breites Maßnahmenpaket in die Wege geleitet hat, das diesbezüglich Abhilfe schaffen soll.⁵

II. Der Cloud and AI Development Act: Ziele und Hebel

Teil dieses Pakets ist auch der Anfang Juni von der Kommission vorgestellte Vorschlag eines „Cloud and AI Development Acts“ (CADA),⁶ mit dem das „Cloud- und KI-Ökosystem“ der EU gestärkt werden soll, um einerseits eine gesteigerte Wettbewerbs- und Innovationsfähigkeit und andererseits eine größere Resilienz und strategische Unabhängigkeit in diesen Bereichen zu erreichen (Art. 1).

Im Dienste dieser Ziele gibt das Gesetz ein breites Spektrum an Maßnahmen vor, die unterschiedliche Ansätze verfolgen und unterschiedliche Hebel nutzbar machen wollen: Sogenannte „Cloud

¹ Antonio Manganelli, Competitiveness, Digital Transformation and EU Policies (CERRE Issue Paper), S. 11.

² Ebenda, S. 15.

³ Ebenda, S. 13.

⁴ Siehe zu den verschiedenen Gefahren „digitaler Abhängigkeit“ bereits den Beitrag im letzten Infobrief, Friedl, Was bedeutet digitale Souveränität für Hochschulen und Universitäten?, DFN-Infobrief Recht 9/2026.

⁵ Siehe beispielsweise European Commission, Joint Communication to the European Parliament and the Council, An International Digital Strategy for the European Union (5. Juni 2026), abrufbar unter <https://digital-strategy.ec.europa.eu/en/library/joint-communication-international-digital-strategy-eu>.

⁶ European Commission, Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act), (2026/0138 (COD)).

and AI Leadership Initiatives“ sollen Ressourcen bündeln, um auf verschiedene Arten und Weisen Forschung und Entwicklung in beiden Bereichen zu fördern (Art. 3-4, 6). Selbiges soll auch auf mitgliedstaatlicher Ebene, eingerahmt von nationalen Cloud- und KI-Strategien (Art. 7), durch sogenannte „Experience and Acceleration Centres for AI“ erfolgen (Art. 5). Von der Kommission ausgewählte „Frontier AI Priority Projects“ sollen privilegierten Zugang zu Rechenressourcen erhalten (Art. 8-9). In von den Mitgliedstaaten einzurichtenden „Data Centre Acceleration Zones“ sollen vereinfachte Genehmigungsprozesse für die Errichtung von Rechenzentren gelten (Art. 10 - 13). Eine neu errichtete „EuroCloud Federation“ soll Behörden vereinfachten Zugang zu Diensten von Rechenzentren und Cloud-Computing-Anbietern geben (Art. 34-36). Außerdem sollen öffentliche Einrichtungen verstärkt Open Source-Angebote nutzen und dafür auch auf einen neuen, von der Kommission bereitgestellten Katalog, zugreifen können (Art. 41-44).

III. Der neue Regelungsrahmen für Cloud-Souveränität

Zentral ist darüber hinaus Kapitel IV des Gesetzes, mit dem ein neuer Rahmen für souveräne Cloud- Computing-Infrastruktur etabliert wird (sogenannte „cloud computing sovereignty framework“). Der Rahmen definiert vier mögliche Stufen der Souveränität für Cloud-Computing-Dienste (Art. 16): Anbieter, die nur Souveränitätslevel 1 erreichen wollen, müssen beispielsweise sicherstellen, dass die gesamte Infrastruktur, die zur Bereitstellung ihrer Dienste in der EU verwendet wird, im Territorium der EU ansässig ist, und alle verarbeiteten Daten zu jedem Zeitpunkt in der EU verbleiben (Annex II, 1.). Für Souveränitätslevel 2 muss darüber hinaus u. a. auch das eingesetzte Personal in der EU ansässig sein und Gewähr dafür bestehen, dass ein Drittstaat, in dessen Jurisdiktion der Anbieter fällt (bspw. die USA im Falle großer amerikanischer Cloud-Anbieter), die Dienstbringung nicht beeinträchtigen und keinen Zugang zu verarbeiteten Daten erhalten kann. Ähnliche Garantien müssen auch bezogen auf die Lieferkette bestehen (Annex II, 2.). Souveränitätslevel 3 verlangt weiter, dass das gesamte eingesetzte Personal Unionsbürgerschaft besitzt; Level 4, dass überhaupt keine Kontrollbeziehung zu einem Drittstaat besteht (Annex II, 3. und 4.). Erst auf Souveränitätslevel 4 sind also Drittstaatsdienste gänzlich ausgeschlossen und kommen nur originär europäische Cloud-Anbieter in Betracht. Für Level 2 bis 4 muss außerdem

eine umfangreiche Konformitätsprüfung durch eine unabhängige Auditororganisation durchlaufen werden (Art. 20-21); für Level 1 reicht eine Selbstzertifizierung (Art. 19).

IV. Cloud-Souveränität als Beschaffungsvoraussetzung

Relevant sollen diese Souveränitätslevel dann insbesondere in der öffentlichen Beschaffung werden: Öffentliche Behörden der EU und der Mitgliedstaaten sollen in Zukunft nur Cloud-Dienste, die mindestens Souveränitätsstufe 1 erfüllen, in Anspruch nehmen dürfen. Außerdem soll alle zwei Jahre jeder Mitgliedstaat bestimmen, welche Behörden, die entweder in die Aufrechterhaltung kritischer Infrastruktur involviert sind oder aber in den Bereichen nationale oder innere Sicherheit, Grenzschutz, Verteidigung, Justiz, Polizei und Strafverfolgung arbeiten, ein höheres Level der Stufen 2 und 3 oder sogar 4 erreichen müssen (Art. 29-30). In außergewöhnlichen Umständen dürfen Behörden festgeschriebene Souveränitätslevel aber auch unterschreiten, etwa wenn die Einhaltung der Vorgaben zu „unverhältnismäßigen Kosten“ führen würde (Art. 30 (4)).

Auf freiwilliger Basis könnten außerdem auch private Akteure, die in den Betrieb kritischer Infrastruktur eingebunden sind, vergleichbare Risikobewertungen ausführen. In Einzelfällen können diese sogar durch die Kommission zur Einhaltung eines bestimmten Souveränitätslevels verpflichtet werden (Art. 31). Schließlich soll die Frage, wie ein bestimmter Anbieter zum Ausbau europäischer Tech-Souveränität beiträgt, auch in allen anderen öffentlichen Beschaffungsverfahren für Cloud-Computing- und KI-Dienste eine Rolle spielen (Art. 31).

V. Auswirkungen in der real-existierenden Cloud-Ökonomie

Es bedarf keines Insiderwissens, um zu verstehen, dass der Souveränitätsrahmen des CADA die Abhängigkeit von den dominanten „Big Three“ der Cloud-Wirtschaft – Google, Microsoft und Amazon Web Services –, die gemeinsam über 70 % des europäischen Marktes kontrollieren, reduzieren soll. Ob dem aber auch in der Praxis so sein wird, erscheint fraglich. Große Cloud-Anbieter haben nämlich schon heute europäische Rechenzentren, mit denen sie die „asset and data localisation“-Anforderungen der

ersten Souveränitätsstufe voraussichtlich einhalten können. Ob die Gefahr des gefürchteten amerikanischen „Kill Switch“,⁷ wie teils behauptet, tatsächlich generell eine Zertifizierung amerikanischer Anbieter in den Stufen 2 und 3 ausschließt, ist offen. Die Kommission selbst geht jedenfalls davon aus, dass für rund sieben von zehn öffentlichen Cloud-Verträgen Souveränitätslevel 1 ausreichend sei und nur für etwa 1 % die höchste Souveränitätsstufe erforderlich sei.⁸

VI. Erste Reaktionen: Lob und leise Zweifel

Von digitalwirtschaftlichen Akteuren wurden der CADA und der darin enthaltene Cloud-Souveränitäts-Rahmen großteils positiv aufgenommen.⁹ Kritische Stimmen blieben aber nicht ganz aus. Befürchtet wird etwa, dass die neuen Nachweis- und Auditierungspflichten für Cloud-Dienste zu übermäßigen Belastungen führen und insbesondere kleine und mittelständische Betriebe ausbremsen könnten. Außerdem steht im Raum, dass die Souveränitätsanforderungen über das hinausgehen, was aus Sicherheitsgründen legitimerweise gefordert werden sollte, und dadurch auch positive Innovation unterbunden werden könnte.¹⁰ Schließlich wird bezweifelt, dass der neue Souveränitätsrahmen an der Dominanz amerikanischer Big-Tech-Dienste viel ändern wird, da wie bereits dargestellt nur auf Souveränitätslevel 4 Drittstaatsdienste definitiv ausgeschlossen sind.¹¹

VII. Hochschulen im CADA: Randnotiz mit Potenzial?

Wird der CADA auch für Universitäten eine Rolle spielen? Das hängt zunächst davon ab, ob Universitäten als „public sector bodies“ i. S. d. Art. 30 CADA gelten werden. Nur für deren Beschaffungsaktivitäten gelten nämlich die Souveränitätsanforderungen. Nach der in Bezug genommenen Definition der Open Data-Richtlinie, die indirekt auch Hochschulen umfasst (Art. 2 Nr. 1 i. V. m. Art. 2 Nr. 4 Open Data-Richtlinie), dürfte das zu bejahen sein. Solange Universitäten aber keine Aufgaben im Bereich der kritischen Infrastruktur oder den anderen gelisteten Hochrisiko-Bereichen wahrnehmen,¹² muss freilich stets nur (das recht permissive) Souveränitätslevel 1 erreicht werden. Dadurch sollte der Compliance-Aufwand bei Hochschulen wohl überschaubar bleiben.

Gleichzeitig bleibt zu hoffen, dass der CADA, wie beabsichtigt, zu einer allgemeinen Vergrößerung und Stärkung der europäischen Cloud-Wirtschaft führen wird. Von dieser würden dann auch Akteure profitieren, die ohne gesetzliche Verpflichtung aus eigenen Stücken sensibles Wissen schützen wollen wie beispielsweise Forschungsinstitutionen. Außerdem könnten auch die übrigen vom CADA vorgeschlagenen Entwicklungstreiber positive Folgen für den Wissenschaftsbereich zeitigen, beispielsweise indem Wissenschaftsakteure erleichtert auf hoch entwickelte Cloud-Dienste zurückgreifen können oder von Finanzierungsgeldern für deren Entwicklung profitieren.¹³ Dass der CADA den Hochschulbereich nur in einem einzigen Nebenpunkt anspricht – nach Art. 5 Abs. 3 lit. c sollen die von den Mitgliedstaaten einzurichtenden Experience and Acceleration Centres for AI das

7 Im Kontext der digitalen Souveränität bezeichnet „Kill Switch“ (Notausschalter) das Risiko, dass ausländische Tech-Konzerne oder deren Regierungen den Zugriff auf Software, Daten oder Cloud-Dienste für europäische Nutzer abrupt sperren oder abschalten; siehe zum Begriff bereits Friedl, Was bedeutet digitale Souveränität für Hochschulen und Universitäten?, DFN-Infobrief Recht 9/2026.

8 Théophane Hartmann, Commission's sovereign cloud plan doesn't push US hyperscalers out (Euractiv, 3. Juni 2026), abrufbar unter <https://www.euractiv.com/news/commissions-sovereign-cloud-plan-doesnt-push-us-hyperscalers-out/>.

9 Etwa European Data Centre Association, Feedback EU Cloud and AI Development Act, abrufbar unter: <https://www.eudca.org/eudca-feedback-eu-cloud-and-ai-development-act>; Bundesverband mittelständische Wirtschaft, Stellungnahme zum Cloud and AI Development Act, abrufbar unter <<https://www.bvmw.de/de/internet-und-digitalisierung/news/stellungnahme-zum-cloud-and-ai-development-act>.

10 Business Software Alliance, BSA Raises Concerns About Key Elements of the EU Cloud and AI Development Act, abrufbar unter <https://www.bsa.org/news-events/news/bsa-raises-concerns-about-key-elements-of-the-eu-cloud-and-ai-development-act>.

11 Article 19, Sovereignty washing: a critical reading of EU's Tech Sovereignty Package, abrufbar unter <https://www.article19.org/resources/sovereignty-washing-a-critical-reading-of-eus-tech-sovereignty-package/>.

12 Siehe bereits oben.

13 Der CADA spricht diese Dimension selbst freilich nur in einem Punkt an: Nach Art. 5 Abs. 3 lit. c sollen die von den Mitgliedstaaten einzurichtenden Experience and Acceleration Centres for AI das Scaling-Up von universitären Ausgründungen und Start-Ups unterstützen.

Scaling-Up von universitären Ausgründungen und Start-ups unterstützen – könnte sich natürlich auch noch ändern. Mit dem Kommissionsvorschlag hat das Gesetzgebungsverfahren gerade erst begonnen. Weitere Impulse von Stakeholdern und den beiden anderen Gesetzgebern – Europäisches Parlament und Rat – werden sicher noch zu Änderungen führen.

Was ändert der KI-Omnibus?

Die finale Version des KI-Omnibusses ist in Kraft getreten

Von Philipp Schöbel

Am 24. Juli 2026 wurde im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz die Digital-Omnibus-Verordnung zur KI (KIO-VO) im Amtsblatt der EU veröffentlicht. Sie trat am 27. Juli 2026 in Kraft und bringt zahlreiche Änderungen mit sich, die teilweise bereits im Kommissionsentwurf (Komm-E)¹ enthalten waren. Im Laufe des Gesetzgebungsverfahrens sind aber auch neue Regelungen hinzugekommen. Einige dieser Änderungen haben auch Auswirkungen auf Hochschulen und Forschungseinrichtungen.

I. Einleitung

Die EU ist bestrebt, eine ganze Reihe von Rechtsakten zu überarbeiten und in mehreren Bereichen bestehende regulatorische Defizite durch Reformen auszugleichen.² Dies geschieht in sogenannten Omnibus-Paketen. Diese mittlerweile zwölf Pakete sind thematisch gegliedert.³ Die Digital-Omnibus-Verordnung zur KI ist Teil des Omnibus-Pakets VII („Digitales“), das zwei Gesetzgebungsvorhaben umfasst. Das „Omnibus-Paket VII: Digitales“ umfasst neben der „Digital-Omnibus-Verordnung“⁴ die „Digital-Omnibus-Verordnung zur KI“ (KIO-VO)⁵. Beide Gesetzgebungsvorhaben sollen jeweils mehrere bestehende

Sekundärrechtsakte ändern. Grund für die Aufteilung in zwei Verordnungen ist insbesondere, dass die KIO-VO zeitkritische Änderungen am Geltungsbeginn der KI-VO vorsieht.⁶

Ziel der Digital-Omnibus-Verordnung ist vor allem eine Angleichung und Reform europäischer Datenrechtsakte.⁷ Für diesen zweiten Teil des Omnibus-Pakets VII ist bisher noch keine politische Einigung erzielt worden. Anders ist dies hinsichtlich des Verordnungsentwurfs der Europäischen Kommission aus dem November 2025 für den KI-Omnibus. Dieser zielte vor allem auf Änderungen der KI-VO ab.⁸ Nachdem das Europäische Parlament im März 2026 Änderungen des Kommissionsentwurfs

1 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), COM(2025)836 final, abrufbar unter: <https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:52025PC0836>.

2 Vgl. Borges, CR 2026, 131.

3 Zur Übersicht zu den unterschiedlichen Omnibus-Paketen siehe: Europäischer Rat, Vereinfachung der EU-Vorschriften, abrufbar unter: <https://www.consilium.europa.eu/de/policies/simplification/>; alle Internetquellen zuletzt abgerufen am 26. August 2026.

4 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 und der Richtlinien 2002/58/EG, (EU) 2022/2555 und (EU) 2022/2557 hinsichtlich der Vereinfachung des digitalen Rechtsrahmens und zur Aufhebung der Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, und der Richtlinie (EU) 2019/1024 (Digital-Omnibus-Verordnung), COM(2025) 837 final.

5 Verordnung (EU) 2026/1744 des Europäischen Parlaments und des Rates vom 8. Juli 2026 zur Änderung der Verordnungen (EU) 2024/1689, (EU) 2018/1139 und (EU) 2023/1230 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), ABl. L, 2026/1744, 24.7.2026.

6 Borges, CR 2026, 131.

7 Zur Digital-Omnibus-Verordnung siehe: Müller, Alles bleibt anders, DFN-Infobrief Recht 2/2026, S. 6-9.

8 Schöbel, Die KI-VO im Omnibus, DFN-Infobrief Recht 2/2026, S. 2-5.

vorgeschlagen hatte (EP-Entwurf),⁹ erfolgte die Einigung über die Änderungen an der Verordnung im Mai und die Verordnung wurde nach erfolgreichem Abschluss des europäischen Rechtssetzungsverfahrens im Juli im Amtsblatt veröffentlicht.

II. Neue verbotene KI-Praktiken

Mit der KIO-VO werden zwei neue Verbote in die KI-VO eingefügt, die jeweils im Komm-E noch nicht vorgesehen waren. Das erste Verbot betrifft sogenannte „Nudify-Apps“.¹⁰ Verboten sind demnach nun das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das nicht einvernehmliche sexuell explizite und intime Inhalte erstellt oder manipuliert (Art. 5 Abs. 1 UAbs. 1 lit. ba KI-VO). Das zweite Verbot umfasst das Inverkehrbringen, die Inbetriebnahme oder die Verwendung eines KI-Systems, das Material über sexuellen Kindesmissbrauch erzeugt oder manipuliert (Art. 5 Abs. 1 UAbs. 1 lit. bb KI-VO). Beide Verbote können sich auch aus anderen Rechtsvorschriften der EU oder der Mitgliedstaaten ergeben.¹¹ Sie gelten nach Art. 113 Abs. 3 lit. a KI-VO ab dem 2. Dezember 2026.

Allerdings werden Ausnahmen für diese beiden Verbote eingefügt (Art. 1 Nr. 7 KIO-VO iVm Art. 5 Abs 1a KI-VO). Grund dafür ist, dass die Weiterentwicklung von KI-Systemen zur Erzeugung oder Manipulation von Videos oder Audiodateien möglich sein soll.¹² Daher sind das Inverkehrbringen oder die Inbetriebnahme nur in zwei Fällen verboten. Der erste Fall ist dann einschlägig, wenn die Erzeugung oder Manipulation die Zweckbestimmung des KI-Systems sind (Art. 5 Abs. 1a lit. a Ziff. i KI-VO). Der zweite Fall umfasst KI-Systeme, die ohne erhebliche technische Änderungen solches Material reproduzierbar erstellen können und nicht über angemessene technische Sicherungsmaßnahmen verfügen (Art. 5 Abs. 1a lit. a Ziff. ii KI-VO). Die zweite Ausnahme bezieht sich auf die Verwendung solcher KI-Systeme. Daher ist es nur verboten, diese KI-Systeme zu verwenden, wenn der/

die Betreiber:in das System zum Zwecke der Erzeugung oder der Manipulation solchen Materials oder solcher Darbietungen verwendet (Art. 5 Abs. 1a lit. b KI-VO).

III. KI-Kompetenz

Während der Komm-E noch eine Abschaffung der Pflicht zur KI-Kompetenz¹³ vorsah (Art. 1 Nr. 4 EU-Komm),¹⁴ wird diese nun erhalten, aber abgewandelt. Die neue Regelung verpflichtet Anbieter:innen und Betreiber:innen von KI-Systemen weiterhin dazu, Maßnahmen zur Förderung der KI-Kompetenz ihrer Mitarbeitenden sowie anderer Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, zu ergreifen (Art. 4 Abs. 1 S. 2 KI-VO). Allerdings müssen sie nicht für das Niveau der KI-Kompetenz einzelner Personen garantieren (Art. 4 Abs. 1 S. 2 KI-VO). Im Endeffekt werden Hochschulen und Forschungseinrichtungen ihre bereits eingeführten Schulungsmaßnahmen demnach voraussichtlich nicht grundlegend ändern müssen.

Weiterhin werden jetzt die EU und ihre Mitgliedstaaten in die Förderung von KI-Kompetenz eingebunden. Die Kommission und die Mitgliedstaaten haben die Aufgabe, die Anbieter:innen und Betreiber:innen von KI-Systemen hinsichtlich der Förderung von KI-Kompetenz zu unterstützen und ihre entsprechenden Bemühungen zu erleichtern (Art. 4 Abs. 2 S. 1 KI-VO). Dies gilt insbesondere für kleine und mittlere Unternehmen (Art. 4 Abs. 2 S. 1 KI-VO).

IV. Registrierung in der EU-Datenbank

Anbieter:innen müssen ihre anwendungsbezogenen Hochrisiko-KI-Systeme (Art. 6 Abs. 2 iVm Anhang III KI-VO) in einer

9 Europäisches Parlament, Abänderungen des Europäischen Parlaments vom 26. März 2026 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnungen (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI) (COM(2025)0836 – C10-0304/2025 – 2025/0359(COD)), abrufbar unter: [https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2026/03-26/0098/P10_TA\(2026\)0098_DE.pdf](https://www.europarl.europa.eu/RegData/seance_pleniere/textes_adoptes/definitif/2026/03-26/0098/P10_TA(2026)0098_DE.pdf).

10 Vgl. Erwg. Nr. 11 KIO-VO.

11 Vgl. Erwg. Nr. 15 KIO-VO.

12 Vgl. Erwg. Nr. 12 KIO-VO.

13 Zur ursprünglichen Pflicht zur KI-Kompetenz siehe: Schöbel, KI-Kompetente Hochschulen, DFN-Infobrief Recht 08/2025, S. 7-10.

14 Vgl. Borges, CR 2026, 132.

EU-Datenbank registrieren (Art. 16 lit. i iVm Art. 49 Abs. 1 KI-VO). Dies müssen sie auch dann, wenn sie sich auf eine Ausnahmeregelung berufen (Art. 6 Abs. 3 KI-VO) und ihr KI-System als nicht hochriskant einstufen (Art. 6 Abs. 4 S. 2 iVm Art. 49 Abs. 2 KI-VO). Der Komm-E sah vor, die Registrierung von KI-Systemen, die unter die Ausnahme des Art. 6 Abs. 3 KI-VO fallen, zu streichen (Art. 1 Nr. 14 EU-Komm).¹⁵ Die Registrierungspflicht wurde indes beibehalten. Jedoch wurden Vereinfachungen für die Registrierung in der EU-Datenbank (Art. 71 KI-VO) eingeführt. Die bei der Registrierung in der EU-Datenbank bereitzustellenden Informationen sind im Anhang VIII KI-VO aufgeführt. Einzelne dieser Anforderungen wurden nun gestrichen (Art. 1 Nr. 2 KIO-VO). Soweit Hochschulen und Forschungseinrichtungen sich auf die Ausnahme des Art. 6 Abs. 3 KI-VO berufen, müssen sie daher als Anbieter:innen ihre KI-Systeme weiterhin in der EU-Datenbank registrieren.

V. Verhältnis zwischen KI-VO und sektoralem Produktsicherheitsrecht

Eine weitere Änderung betrifft das Verhältnis von KI-VO und anderen sektoralen, produktbezogenen Rechtsakten. Grundsätzlich wird bei produktbezogenen Hochrisiko-KI-Systemen (Art. 6 Abs. 1 iVm Anhang I KI-VO) zwischen zwei Kategorien unterschieden. Für Hochrisiko-KI-Systeme, die unter die in Anhang I Abschnitt A KI-VO aufgeführten Rechtsakte fallen, gelten sowohl die Anforderungen der KI-VO als auch die Anforderungen aus dem jeweils einschlägigen Rechtsakt. Für solche Hochrisiko-KI-Systeme, die unter die Rechtsakte des Anhang I Abschnitt B KI-VO fallen, gelten die meisten Anforderungen der KI-VO nicht direkt (Art. 2 Abs. 2 S. 1 KI-VO). Die Anforderungen der KI-VO werden aber in die jeweiligen Rechtsakte integriert. Für jeden Rechtsakt des Anhang I Abschnitt B enthält die KI-VO daher eine Regelung, wie die Vorschriften über Hochrisiko-KI-Systeme aus der KI-VO in das Regelwerk des jeweiligen Rechtsakts inkorporiert werden (Art. 102-112).

Der EP-Entwurf sah vor, dieses zweite System auf den gesamten Anhang I KI-VO auszuweiten. Danach sollten alle in Anhang I

Abschnitt A KI-VO aufgeführten Rechtsakte in Abschnitt B transferiert und für jeden dieser Rechtsakte eigene Regelungen für die Integration der Vorschriften über Hochrisiko-KI-Systeme in die jeweiligen Rechtsakte geschaffen werden (Abänderung 75, 81, 82 EP-Entwurf). Nach der finalen Einigung wird nun nur die Maschinen-Verordnung (MVO)¹⁶ von Anhang I Abschnitt A in Abschnitt B KI-VO verschoben und die MVO so angepasst, dass die Anforderungen an Hochrisiko-KI-Systeme in die MVO integriert werden. Hierzu wird der Kommission in Art. 8 Abs. 3 MVO eine Befugnis zum Erlass delegierter Rechtsakte eingeräumt. Für das Verhältnis der restlichen noch in Anhang I Abschnitt A KI-VO aufgeführten Rechtsakte zur KI-VO wurde eine flexible Lösung gefunden. Zukünftig kann die Anwendung der Anforderungen und Pflichten für produktbezogene Hochrisiko-KI-Systeme, die unter Anhang I Abschnitt A KI-VO fallen, beschränkt werden. Dafür muss zum einen das Schutzniveau in Bezug auf Gesundheit, Sicherheit oder Grundrechte in diesen Rechtsakten genauso hoch wie in der KI-VO oder höher sein (Art. 2 Abs. 13 UAbs. 1 lit. a KI-VO). Zum anderen darf aber auch das Schutzniveau der KI-VO dadurch nicht verringert werden (Art. 2 Abs. 13 UAbs. 1 lit. b KI-VO). Dies wird durch die Kommission im Wege delegierter Rechtsakte konkretisiert (Art. 2 Abs. 13 UAbs. 2 KI-VO).

VI. Mehr Aufsichtsbefugnisse für das KI-Büro

Das Büro für künstliche Intelligenz (KI-Büro) ist Teil der Europäischen Kommission. Es beschäftigt derzeit ca. 125 Mitarbeitende und verfügt über sechs Referate sowie zwei Berater.¹⁷ Ihm standen bereits nach der ursprünglichen KI-VO umfassende Aufsichtsbefugnisse zu. Es hat etwa eine ausschließliche Zuständigkeit für die Beaufsichtigung und Durchsetzung der Pflichten der Anbieter:innen von KI-Modellen mit allgemeinem Verwendungszweck (Art. 88 Abs. 1 KI-VO).¹⁸

Für den Fall, dass ein KI-System auf einem KI-Modell mit allgemeinem Verwendungszweck beruhte und Modell sowie System von dem/derselben Anbieter:in entwickelt wurden, war das KI-Büro befugt, die Konformität des KI-Systems mit den Pflichten aus

¹⁵ Vgl. Borges, CR 2026, 135; Pilz, KIR 2026, 146, 149 f.

¹⁶ Verordnung (EU) 2023/1230 des Europäischen Parlaments und des Rates vom 14. Juni 2023 über Maschinen und zur Aufhebung der Richtlinie 2006/42/EG des Europäischen Parlaments und des Rates und der Richtlinie 73/361/EWG des Rates, ABl. L 165 vom 29.6.2023, S. 1.

¹⁷ EU-Komm., Europäisches KI-Büro, abrufbar unter: <https://digital-strategy.ec.europa.eu/de/policies/ai-office>.

¹⁸ Siehe dazu bereits: Schöbel, KI-Modelle made in Europe?, DFN-Infobrief Recht 4/2025, S.19.

dieser Verordnung zu überwachen und zu beaufsichtigen (Art. 75 Abs. 1 KI-VO a.F.). Dies wurde nun zu einer ausschließlichen Zuständigkeit ausgeweitet (Art. 1 Nr. 31 KIO-VO). Jedoch gibt es vier Ausnahmen von dieser ausschließlichen Zuständigkeit. Die erste dieser Ausnahmen besteht für KI-Systeme, die unter die in Anhang I KI-VO aufgeführten produktsicherheitsrechtlichen Rechtsakte fallen (Art. 75 Abs. 1 UAbs. 1 lit. a Ziff. i KI-VO). Eine weitere Ausnahme gilt für Hochrisiko-KI-Systeme, die im Bereich der kritischen Infrastruktur eingesetzt werden (Art. 75 Abs. 1 UAbs. 1 lit. a Ziff. ii KI-VO). Darüber hinaus sind solche KI-Systeme ausgenommen, die von Strafverfolgungsbehörden, Grenzverwaltungsbehörden und Finanzinstituten bereitgestellt werden (Art. 75 Abs. 1 UAbs. 1 lit. a Ziff. iii KI-VO). Schließlich sind auch solche Hochrisiko-KI-Systeme ausgenommen, die im Bereich der Rechtspflege eingesetzt werden (Art. 75 Abs. 1 UAbs. 1 lit. a Ziff. iv KI-VO). Eine vergleichbare Ausnahme für den Hochschulsektor gibt es indes nicht. Zudem ist das KI-Büro nun ausschließlich zuständig für KI-Systeme, die sehr große Online-Plattformen oder sehr große Online-Suchmaschinen i. S. d. Art. 33 Abs. 1 Digital Services Act (DSA)¹⁹ bilden oder in diese integriert sind (Art. 75 Abs. 1 Abs. 1 lit. b KI-VO).

VII. Ausblick

Im finalen Verordnungstext finden sich viele Vorschläge der Kommission wieder. So ist etwa die Erlaubnis zur Verarbeitung besonderer Kategorien personenbezogener Daten zur Erkennung und Korrektur von Verzerrungen (Bias) ausgeweitet worden. Im ursprünglichen Normtext der KI-VO galt diese Erlaubnis nur für Anbieter:innen von Hochrisiko-KI-Systemen (Art. 10 Abs. 5 KI-VO a.F.). Zukünftig dürfen sich auch Betreiber:innen von Hochrisiko-KI-Systemen sowie Anbieter:innen und Betreiber:innen von KI-Modellen und KI-Systemen, die keine Hochrisiko-KI-Systeme sind, unter strengen Voraussetzungen auf diese Ausnahme berufen (Art. 4 a Abs. 2 KI-VO).

Weiterhin wurden auch die Maßnahmen zur Innovationsförderung²⁰ ausgeweitet. So kann etwa zukünftig auch das KI-Büro

(Art. 3 Nr. 47 KI-VO) ein KI-Reallabor für solche KI-Systeme einrichten, für deren Aufsicht es nach Art. 75 Abs. 1 KI-VO zuständig ist (Art. 57 Abs. 3a S. 1 KI-VO). Auch können zukünftig neben anwendungsbezogenen Hochrisiko-KI-Systemen (Art. 6 Abs. 2 iVm Anhang III KI-VO) auch produktbezogene Hochrisiko-KI-Systeme (Art. 6 Abs. 1 iVm Anhang I KI-VO) unter Realbedingungen außerhalb von KI-Reallaboren getestet werden (Art. 60 Abs. 1 UAbs. 1 KI-VO).

Für Hochschulen dürfte zudem relevant sein, dass der Geltungsbeginn der Vorschriften zu Hochrisiko-KI-Systemen verschoben wurde. Zukünftig sollen die Pflichten für anwendungsbezogene Hochrisiko-KI-Systeme (Art. 6 Abs. 2 iVm Anhang III KI-VO) ab dem 2. Dezember 2027 gelten (Art. 113 UAbs. 3 lit. c Ziff. i KI-VO). Für produktbezogene Hochrisiko-KI-Systeme (Art. 6 Abs. 1 iVm Anhang I KI-VO) werden die Pflichten sogar erst ab dem 2. August 2028 gelten (Art. 113 UAbs. 3 lit. c Ziff. i KI-VO). Zu beachten ist allerdings, dass die neuen Verbote nach Art. 5 Abs. 1 UAbs. 1 lit. ba und bb sowie Art. 5 Abs. 1a und 1b KI-VO bereits ab dem 2. Dezember 2026 gelten. Weiterhin wird die Geltung der Transparenzpflichten²¹ für Anbieter:innen von bereits in Verkehr gebrachten KI-Systemen auf den 6. Dezember 2026 gelegt (Art. 111 Abs. 4 KI-VO, Art. 1 Nr. 39 KIO-VO). Insgesamt verschafft der KI-Omnibus auch dem Hochschulsektor mehr Zeit bei der Implementierung der KI-VO.

¹⁹ Zu den Vorschriften des DSA zu sehr großen Online-Plattformen oder sehr großen Online-Suchmaschinen siehe: von Bernuth, Systemische Risiken riesiger Systeme, DFN-Infobrief Recht 9/2024, S. 1-6.

²⁰ Zu den Instrumenten der Innovationsförderung in der KI-VO siehe: Schöbel, Europäische Sandkästen für KI, DFN-Infobrief Recht 8/2024, S. 2-6.

²¹ Zu den Transparenzpflichten für Anbieter:innen und Betreiber:innen von KI-Systemen siehe: Friedl, Mit digitalen Wasserzeichen zu klareren Informationsökosystemen?, DFN-Infobrief Recht 5/2026, S. 2-5.

DFN Infobrief-Recht-Aktuell

- **Datenschutzrecht: noyb mahnt SCHUFA wegen Speicherung historischer Daten ab**

Die SCHUFA speichert nach eigenen Angaben einen gesonderten Datenbestand zu Verbrauchern, der nicht mehr in die reguläre Scoreberechnung einfließt. Sie hält diese Speicherung unter anderem zur Qualitätssicherung und Überprüfung von Scoring-Verfahren für zulässig. Die Datenschutzorganisation noyb kritisiert diese Praxis und vertritt die Auffassung, dass die Daten nach Ablauf der maßgeblichen Speicherfrist gelöscht werden müssten. Darüber hinaus beanstandet noyb, dass die betreffenden Daten nicht vollständig im Rahmen von Auskunftersuchen nach Art. 15 DSGVO offengelegt würden. noyb ist der Auffassung, dass Betroffene Zugänge zu sämtlichen über sie gespeicherten personenbezogenen Daten erhalten müssten. noyb hat die SCHUFA deshalb nach eigenen Angaben abgemahnt. Zudem hat noyb angekündigt, eine Unterlassungsklage zu erheben. Darüber hinaus soll geprüft werden, ob Schadensersatzansprüche für Personen geltend gemacht werden können, die aufgrund unvollständiger Auskünfte in ihren Rechten verletzt wurden.

Hier erhalten Sie die Links zur Pressemitteilung von noyb (alle Links dieser Seite wurden zuletzt am 16.09.2026 abgerufen):

<https://noyb.eu/de/shadow-database-scandal-noyb-sends-schufa-cease-and-desist-letter-interest-list-class-action>

Hier erhalten Sie die Links zur Pressemitteilung der SCHUFA:

<https://www.schufa.de/newsroom/bonitaet/schufa-datenbestand/index.jsp>

- **Telekommunikationsrecht: HateAid stellt Strafanzeige wegen Smart Glasses**

Smart Glasses ermöglichen unter anderem Foto- und Videoaufnahmen über unauffällige integrierte Kameras. Dadurch können Personen unter Umständen unbemerkt aufgenommen und die Aufnahmen anschließend verbreitet werden. Die gemeinnützige Organisation HateAid hat daher Mitte August bei der Zentralstelle zur Bekämpfung der Internet-kriminalität (ZIT) Strafanzeige gegen die Geschäftsführung mehrerer Unternehmen gestellt. Nach Auffassung von HateAid verstößt der Vertrieb bestimmter Smart Glasses gegen § 8 Abs. 1 i.V.m. § 27 Abs. 1 Nr. 3 TDDDG. Danach ist es verboten, als Alltagsgegenstände getarnte Telekommunikationsanlagen auf den Markt zu bringen, die dazu bestimmt und geeignet sind, andere unbemerkt aufzunehmen.

Hier erhalten Sie den Link zur Pressemitteilung:

<https://hateaid.org/hateaid-stellt-strafanzeige-gegen-meta-wegen-smart-glasses/>

- **Datenschutzrecht: Datenschutzkonferenz (DSK) veröffentlicht Eckpunktepapier zur Modernisierung des Datenschutzrechts**

Die Datenschutzkonferenz hat das Eckpunktepapier „Stuttgarter Impulse zur Modernisierung des Datenschutzrechts“ verabschiedet. Darin sprechen sich die unabhängigen Datenschutzaufsichtsbehörden der Länder gegen eine Zentralisierung der Datenschutzaufsicht und insbesondere gegen eine Übertragung ihrer Zuständigkeiten auf die Bundesdatenschutzbeauftragte für den Datenschutz und Informationsfreiheit aus:

Hier erhalten Sie den Link zur Pressemitteilung der DSK:

https://www.datenschutzkonferenz-online.de/media/en/20260619_Entschliessung_Stuttgarter-Impulse-zur-Modernisierung-des-Datenschutzes.pdf

Kurzbeitrag: EU-Chatkontrolle - Totgesagte leben länger

Die europäischen Gesetzgeber wollen es Betreibern privater Messaging-Dienste jetzt doch erlauben, nach Darstellungen von Kindesmissbrauch zu suchen

Von Dr. Paul Friedl

Der europäische Vorschlag für eine sogenannte Chatkontrolle, mit der Messenger-Betreiber auch private Chats nach Missbrauchsmaterial durchsuchen dürften, schien endgültig vom Tisch. Doch jetzt hat das Parlament das Projekt überraschend doch gebilligt. Sind bald auch verschlüsselte Chats gläsern?

I. Die EU-Chatkontrolle: Eine unendliche Geschichte

Die Verbreitung von Darstellungen sexuellen Kindesmissbrauchs – im Fachdiskurs gewöhnlich als Child Sexual Abuse Material (CSAM) betitelt – stellt eines der schwerwiegendsten Verbrechen dar, für dessen Begehung digitale Kommunikationsdienste regelmäßig verwendet werden. Schon seit Ende der Nullerjahre führten viele Tech-Konzerne, angeführt von Google, technologische Infrastrukturen ein, mit denen von Nutzer:innen verbreitete Missbrauchsdarstellungen durch Abgleich mit bekanntem Missbrauchsmaterial identifiziert und an die Strafverfolgungsbehörden weitergeleitet werden können. Mit dem Aufstieg des Web 2.0 begannen dann auch Social-Media-Plattformen, Inhalte zu scannen. Facebook etwa gab 2018 bekannt, dass es auch alle über die Chat-Funktion „Facebook Messenger“ verschickten Daten auf CSAM überprüft.¹

Die Verabschiedung des Europäischen Kodex für die elektronische Kommunikation,² mit dem auch Messenger- und E-Mail-Dienste den Regeln der ePrivacy-Richtlinie³ unterworfen wurden, machte diese Praxis 2020 rechtlich problematisch. Da politisch aber gewollt war, dass Diensteanbieter freiwillig weiter nach Missbrauchsmaterial suchen könnten, verabschiedete die EU im Juli 2021 die sogenannte Interimsverordnung (EU) 2021/1232, die Online-Diensten unter bestimmten Voraussetzungen und befristet bis August 2024 die Verarbeitung von Kommunikationsinhalten und Verkehrsdaten zur Erkennung von Missbrauchsmaterial und somit die Kontrolle eigentlich „unantastbarer“ privater Kommunikation erlaubte (sogenannte „Chatkontrolle 1.0“).⁴ Die Geltungsdauer dieser Regelung wurde 2024 bis zum 3. April 2026 verlängert.

Gleichzeitig legte die Kommission erstmals im Mai 2022 einen Vorschlag für eine sogenannte CSA-Verordnung (engl. Child

¹ Times Herald, Facebook admits it scanned Messenger to detect 'images of child exploitation and malware' (5. April 2018), abrufbar unter <https://www.timesheraldonline.com/2018/04/05/facebook-admits-it-scanned-messenger-to-detect-images-of-child-exploitation-and-malware/>.

² Richtlinie (EU) 2018/172 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

³ Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

⁴ Befürworter der Idee lehnen den Begriff „Chat-Kontrolle“ als Kampfbegriff ab.

Sexual Abuse Regulation, sogenannte „Chatkontrolle 2.0“⁵ vor. Mit dieser sollten Anbieter von Hosting-Diensten sowie öffentlich zugänglichen interpersonellen Kommunikationsdiensten unter bestimmten Voraussetzungen durch sogenannte Aufdeckungsanordnungen dazu verpflichtet werden können, Anti-CSAM-Technologien einzusetzen. Der Verordnungsvorschlag war ausdrücklich technologieneutral ausgestaltet und hätte daher auch die Kontrolle mithilfe sogenannter Client-Side-Scannings, durch Analyse noch nicht verschlüsselter Inhalte lokal auf dem Absendegerät, ermöglicht. Erfasst werden sollten dabei auch Anbieter Ende-zu-Ende verschlüsselter Kommunikationsdienste.⁶ Nach Vorlage des Kommissionsvorschlags wurde dieser im Laufe der Verhandlungen mehrfach verändert und in Teilen abgeschwächt. Über mehrere Jahre konnte sich der Rat jedoch nicht auf eine gemeinsame Verhandlungsposition verständigen. Erst im November 2025 einigte er sich auf eine solche Position.⁷ Die endgültige Fassung muss jedoch zwischen Rat, Parlament und Kommission im sogenannten Trilog-Verfahren ausgehandelt werden. Hier steht eine Einigung aber noch aus, sodass das Gesetzgebungsverfahren noch nicht abgeschlossen ist und die CSA-Verordnung bisher noch nicht Realität geworden ist.⁸

Anfang April 2026 sollte die Ausnahmeregelung für die freiwillige Chatkontrolle (Chatkontrolle 1.0) dann auslaufen. Und tatsächlich fanden EU-Parlament und Rat keinen Kompromiss, mit dem die vorübergehende Ausnahmeregelung für Diensteanbieter

verlängert worden wäre. Dem Vorschlag des Parlaments, die Kontrolle auf Fälle zu beschränken, in denen Justizbehörden einzelne Verdächtige oder Gruppen von Verdächtigen zuvor als legitimes Überwachungsziel bestimmt hatten, und verschlüsselte Kommunikationsdienste von der Ausnahmeregelung auszunehmen, wollte der Rat nicht zustimmen.⁹ Die Verhandlungen führten deshalb zu keiner Einigung und die Ausnahmeregelung lief am 3. April 2026 aus.

II. Showdown und Entscheidung im Juli

Obwohl das Parlament seine Position also eigentlich deutlich gemacht hatte, legte der Rat auf Anregung der Parlamentspräsidentin Roberta Metsola im Juni einen weiteren Vorschlag für die Übergangsregelung vor.¹⁰ Gleichzeitig beantragte die Europäische Volkspartei (EVP) ein Eilverfahren, um noch vor der Sommerpause über den Vorschlag abstimmen zu können, der angenommen wurde.¹¹ In der damit erzwungenen zweiten Abstimmung über den Ratsentwurf¹² brauchte es die absolute Mehrheit der Mitglieder des Parlaments, um den Ratsentwurf zurückzuweisen. Auch weil viele Parlamentarier schon in der Sommerpause waren, konnte sich hier die EVP-Position mit teilweiser Unterstützung der Europäischen Sozialdemokraten durchsetzen. In der entscheidenden Abstimmung am 9. Juli 2026 stimmten zwar mehr Abgeordnete für eine Ablehnung

5 Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse (COM/2022/209 final); siehe zu diesem Vorschlag und den Entwicklungen bis Februar 2024 bereits Voget, Vertrauen ist gut – Überwachung ist besser?, DFN-Infobrief Recht 2 / 2024, S. 11.

6 Der damalige Bundesdatenschutzbeauftragte Ulrich Kelber sprach sich zur Zeit, wie viele andere Datenschützer:innen, gegen den Kommissionsentwurf aus. Die „Durchleuchtung sämtlicher privater Nachrichteninhalte ist keine Option“; Überwachungen, die nicht auf einen spezifischen Verdacht beruhen, seien „der Einstieg in eine anlasslose Massenüberwachung“, Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Pressemitteilung 1/2024 (14. Februar 2024), abrufbar unter https://www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2024/01_CSA-Verordnung.html.

7 Council of the European Union, Interinstitutional File 2022/0155 (COD).

8 Siehe weiter unten Teil. III.

9 European Digital Rights (EDRI), Did the EU Parliament really vote not to protect children online? (11. Mai 2026), abrufbar unter <https://edri.org/our-work/did-the-eu-parliament-really-vote-not-to-protect-children-online/>.

10 LTO-Redaktion, Die Chatkontrolle kommt doch (9. Juli 2026), abrufbar unter <https://www.lto.de/recht/nachrichten/n/bekaempfung-von-kinderpornografie-chatkontrolle-eu-parlament-scan-erlaubnis>.

11 Ebenda.

12 Für gewöhnlich kommt es bei einer Ablehnung eines Ratsentwurfs durch das Parlament, wie sie hier schon geschehen war, nicht zu einer zweiten Abstimmung im Parlament, sondern zur Durchführung des Trilog-Verfahrens, sh. Euronews, Europa-Parlament: EVP-Manöver bringt Chat-Kontrolle gegen Kindesmissbrauch zurück (7. Juli 2026), abrufbar unter <https://de.euronews.com/my-europe/2026/07/07/europa-parlament-evp-manover-bringt-chat-kontrolle-gegen-kindesmissbrauch-zurueck>.

des Ratsstandpunkts als dagegen. Die erforderliche Mehrheit von 360 Stimmen wurde jedoch verfehlt.¹³ Für das äußerst ungewöhnliche Vorgehen erhielten EVP und Parlamentspräsidentin Metsola scharfe Kritik.¹⁴

Mittel im Kampf gegen sexuelle Ausbeutung und Kindesmissbrauch¹⁷ oder um eine gefährliche Überwachungsstruktur, durch die anlasslos und grundlos privateste Kommunikationswege ausspioniert werden?¹⁸

In der nun abgeseignete Parlamentsposition wurde der letzte Ratsvorschlag nochmals leicht umgearbeitet: Nachrichten, die verschlüsselt werden sollen oder schon verschlüsselt worden sind, sollen nicht kontrolliert werden dürfen.¹⁵ Im Übrigen weicht sie aber nicht mehr von den letzten Rats- und Kommissionsvorschlägen ab – und sieht insbesondere keine Begrenzung auf Verdachtsfälle vor –, sodass mit der noch ausstehenden Zustimmung durch den Rat fest zu rechnen ist. Es kann deshalb davon ausgegangen werden, dass betroffene Dienste bald wieder nach CSAM-Material suchen dürfen – zumindest bis die vorübergehende Ausnahmeregelung im April 2028 wieder abläuft.

III. Die Dauerlösung? Stand der CSA-Verordnung

Gleichzeitig dauern die Verhandlungen über die CSA-Verordnung an. Ob hier ein Kompromiss erreicht werden kann, ist aber immer noch unklar. Zwar hat sich der Rat schon im November 2025 von einer obligatorischen Scan-Pflicht verabschiedet und auch die besondere Schutzbedürftigkeit von verschlüsselter Kommunikation anerkannt.¹⁶ Offen ist aber, ob sich das Parlament auf einen Vorschlag, der keinen Verdachtsbezug voraussetzt und vielmehr auch das freiwillige anlasslose Scannen erlaubt, einlassen wird. Neue Verhandlungsrunden haben im September 2026 begonnen. Gleichzeitig läuft auch die gesellschaftliche Debatte weiter: Handelt es sich bei der „Chatkontrolle“ um ein wichtiges

13 LTO-Redaktion, Die Chatkontrolle kommt doch (9. Juli 2026), abrufbar unter <https://www.lto.de/recht/nachrichten/n/bekaempfung-von-kinderpornografie-chatkontrolle-eu-parlament-scan-erlaubnis>.

14 Für eine Einschätzung, siehe Nicolai von Ondarza, EU Analytics – July 2026 review: Parliament’s self-defeat on “chat control”, and the ECR in limbo (3. August 2026), abrufbar unter <https://www.foederalist.eu/2026/08/eu-analytics-july-2026.html>.

15 Europäisches Parlament, Legislative resolution of 9 July 2026 on the Council position at first reading with a view to the adoption of a regulation of the European Parliament and of the Council on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse (11261/1/2026 – C10 0178/2026 – 2025/0429(COD)).

16 Anna Pinggen, CSAM Regulation: Council Position Reached, EuCrim 4/2025, abrufbar unter: <https://eucrim.eu/news/csa-regulation-council-position-reached/>.

17 Siehe bspw. Internet Watch Foundation, EU Failure on Child Safety: Why CSAM Detection Laws Must Be Restored, abrufbar unter <https://www.iwf.org.uk/policy-work/eu/eu-failure-on-child-safety-why-csam-detection-laws-must-be-restored>.

18 Siehe bspw. Joint statement of scientists and researchers on the EU Presidency’s new proposal for the Child Sexual Abuse Regulation (12. Oktober 2025), abrufbar unter <https://csa-scientist-open-letter.org/Sep2025>.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz. Nachdruck sowie Wiedergabe in elektronischer Form, auch auszugsweise, nur mit schriftlicher Genehmigung des DFN-Vereins und mit vollständiger Quellenangabe.

Herausgeber

Verein zur Förderung eines Deutschen Forschungsnetzes e. V.
DFN-Verein
Alexanderplatz 1, D-10178 Berlin
E-Mail: dfn-verein@dfn.de

Texte:

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der Humboldt-Universität Berlin.

Humboldt-Universität zu Berlin
Lehrstuhl für Bürgerliches Recht und Recht der
Digitalisierung

Prof. Dr. Katharina de la Durantaye, LL. M. (Yale)
Unter den Linden 11, 10117 Berlin

Tel. (030) 838-66754

E-Mail: recht@dfn.de



WEGGEFORSCHT
EIN PODCAST DER FORSCHUNGSSTELLE
RECHT IM DFN

Podcast der Forschungsstelle Recht im DFN

„Weggeforscht“, der Podcast der Forschungsstelle Recht im DFN, informiert knapp und verständlich über relevante juristische Entwicklungen und Fragestellungen im digitalen Umfeld. Neben einem kurzen Newsblock wird in jeder Folge ein aktuelles Thema erörtert.

Er erscheint regelmäßig ein- bis zweimal im Monat auf allen gängigen Podcast-Plattformen.

Link: <https://anchor.fm/fsr-dfn>

