„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht DFN

1/2024
Januar 2024

Geteiltes Wissen ist doppeltes Wissen

Regelungen zur offenen Bereitstellung von Daten durch öffentliche Stellen und Forschungseinrichtungen

Gemeinsam sind wir verantwortlich!

Fehlende Vereinbarung bei gemeinsamer Verantwortung ist ein Bußgeldrisiko

Bist du ein personenbezogenes Datum?

Die Trilogie der europäischen Rechtsprechung zum Personenbezug von Daten

Kurzbeitrag: Risiken und Nebenwirkungen? Jugendgefährdend und gesundheitsschädlich!

US-Bundesstaaten klagen den Meta-Konzern an

Geteiltes Wissen ist doppeltes Wissen

Regelungen zur offenen Bereitstellung von Daten durch öffentliche Stellen und Forschungseinrichtungen

von Johannes Müller

Durch unterschiedliche Regelungen möchte die EU neue Zugangsrechte zu vorhandenen Datensätzen regeln. Insbesondere Daten, die in der Hand öffentlicher Stellen sind, sollen zu fairen Bedingungen weiterverwendet werden können.

I. Die Datenstrategie der EU

Die EU hat erkannt, dass eine innovative Digitalwirtschaft eine große Menge verfügbare Daten erfordert. Heute sind große Datenmengen häufig in der Hand einiger weniger, meist US-amerikanischer, Tech-Unternehmen. Durch bestehende Datenmonopole droht eine Manifestierung und Verstärkung der bereits bestehenden wirtschaftlichen Vormachtstellung der Unternehmen und eine Behinderung des Wettbewerbs. Insbesondere kleinen und mittleren Unternehmen, zu denen auch Start-Ups zählen, fehlt häufig der Zugriff auf bestehende Datensätze, um innovative Produkte zu entwickeln. Die Datenstrategie der EU[1] möchte unter anderem auch auf diese Problemstellung eingehen und neue Datenzugangsrechte gewähren. Gegenüber privaten Akteuren soll der Datenzugang primär im Data Act geregelt werden.[2] Aber auch Daten, die durch die öffentliche Hand generiert wurden, sollen der Allgemeinheit zur Verfügung gestellt werden. Hierzu sehen insbesondere die EU-Richtlinie 2019/1024 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors (PSI-Rl) und der Data Governance-Act Regelungen vor.

II. Datennutzungsregelungen des DNG

Einen essentiellen Baustein zur Nutzung von Daten öffentlicher Stellen bildet das Datennutzungsgesetz (DNG). Das DNG setzt die Regelungen der PSI-Rl um. Durch die Richtlinie soll eine offene Weiterverwendung von Daten gefördert werden, die im Besitz der öffentlichen Hand sind. Indem diese Daten möglichst weitreichend durch die Allgemeinheit genutzt werden können, sollen Innovationen bei Produkten und Dienstleistungen erleichtert werden (Art. 1 Abs. 1 lit. a PSI-Rl). Der deutsche Gesetzgeber hat die PSI-Rl ohne essentielle Änderungen im DNG umgesetzt.

1. Anwendungsbereich des DNG

Durch das DNG werden Datenbereitsteller verpflichtet. Datenbereitsteller im Sinne des DNG sind gemäß § 2 Abs. 2 Nr. 1 DNG primär öffentliche Stellen. Das Gesetz trifft gemäß § 2 Abs. 1 DNG Regelungen zu Daten, die Einzelpersonen oder der Öffentlichkeit bereits zugänglich gemacht wurden. Dies kann der Fall sein, weil die Daten aufgrund eines gesetzlichen Anspruchs auf Zugang (Nr. 1), aufgrund einer gesetzlichen Bereitstellungspflicht (Nr. 2) oder auf sonstige Weise öffentlich oder zur ausschließlichen Nutzung bereitgestellt wurden (Nr. 3). Durch das DNG soll also die Weiterverwendung von Daten geregelt werden, die eine öffentliche Stelle bereits einzelnen Personen oder der Öffentlichkeit zur Verfügung gestellt hat.

§ 2 Abs. 2 Nr. 3 DNG enthält eine eigene Regelung für die Verwendung von Forschungsdaten. Hiernach sind Hochschulen, Forschungseinrichtungen, Forschungsfördereinrichtungen und

1 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen. Eine europäische Datenstrategie, COM (2020) 66 final, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52020DC0066 (zuletzt abgerufen am 05.12.2023).

2 Vgl. Tech, Datenstaat oder Datensalat?, DFN Infobrief 08/2023.

Forschende in Bezug auf Forschungsdaten vom Anwendungsbereich des DNG umfasst, sofern die Forschung öffentlich finanziert wurde und die Forschungsdaten bereits über ein institutionelles oder thematisches Repositorium öffentlich bereitgestellt wurden. Öffentlich finanzierte Forschungsdaten fallen hiernach in den Anwendungsbereich des DNG, sofern sie durch ein Archiv der Öffentlichkeit zugänglich gemacht wurden. Forschungsdaten sind gemäß § 3 Nr. 10 DNG Aufzeichnungen in digitaler Form, die im Laufe wissenschaftlicher Forschungstätigkeiten erfasst werden. Die wissenschaftliche Veröffentlichung selbst ist hiervon nicht umfasst, sondern vielmehr die Daten, die im Forschungsprozess erzeugt wurden.

Auch wenn Forschungseinrichtungen gleichzeitig öffentliche Stellen sein können, stellt die PSI-Rl klar, dass Forschungseinrichtungen lediglich in ihrer Funktion als Forschungseinrichtung und nur in Bezug auf Forschungsdaten von den Regelungen erfasst sind (Erwägungsgrund 28). Öffentlich finanzierte Forschungsdaten sollen standardmäßig der Öffentlichkeit zur Verfügung gestellt werden. Um den Verwaltungsaufwand zu verringern, werden lediglich solche Forschungsdaten geregelt, die bereits über ein institutionelles oder thematisches Archiv öffentlich zugänglich gemacht wurden.

Dennoch ist auch eine Vielzahl von Daten im Besitz öffentlicher Stellen nicht vom Anwendungsbereich des DNG erfasst. Häufig stehen rechtliche Hindernisse einer öffentlichen Weiterverwendung von Daten entgegen. § 2 Abs. 3 DNG nennt eine Vielzahl von Datenkategorien, die nicht vom DNG umfasst sind. So finden die Regelungen etwa keine Anwendung auf Daten, die das geistige Eigentum Dritter betreffen (§ 2 Abs. 3 lit. b DNG). Ebenso kann auch der Schutz personenbezogener Daten einer Weiterverwendung entgegenstehen (§ 2 Abs. 3 lit. a aa)).

2. Grundsatz der uneingeschränkten Datennutzung

Daten, die in den Anwendungsbereich des DNG fallen, sollen nach Möglichkeit uneingeschränkt weitergenutzt werden können. Hierzu normiert § 1 DNG zunächst den Grundsatz der offenen Daten. Soweit möglich sollen hiernach alle Daten im Anwendungsbereich des Gesetzes nach dem Grundsatz „konzeptionell und standardmäßig offen“ erstellt werden. Dies bedeutet, dass Daten in einem offenen Format erstellt werden sollen, die von jeder Person zu jedem Zweck frei weiterverwendet werden können.

Gibt die öffentliche Stelle die Daten weiter, muss sie gemäß § 7 Abs. 1 DNG die Nutzung der Daten in allen angefragten Formaten und Sprachen ermöglichen, die beim Datenbereitsteller auch selbst verfügbar sind. Sofern dies möglich und sinnvoll ist, sollen die Daten gemäß § 7 Abs. 2 DNG elektronisch und in anerkannten offenen, maschinenlesbaren, zugänglichen, auffindbaren und interoperablen Formaten mit den zugehörigen Metadaten bereitgestellt werden. Dies kann die Verwendung der Daten im Rahmen künstlicher Intelligenz erleichtern. Keine Pflicht zur Erstellung von Metadaten besteht gemäß § 7 Abs. 3 DNG, sofern dies mit unverhältnismäßigem Aufwand verbunden ist. Sofern es sich um dynamische Daten handelt, soll gemäß § 8 DNG eine Erfassung in Echtzeit mithilfe geeigneter Schnittstellen ermöglicht werden, sofern der Aufwand und die Kosten nicht unverhältnismäßig sind. Hochwertige Datensätze müssen gemäß § 9 DNG in maschinenlesbarem Format, über geeignete Schnittstellen und, falls technisch möglich, als Massen-Download zur Verfügung gestellt werden. Welche Daten als hochwertig einzuordnen sind, wird gemäß § 3 Nr. 9 DNG durch Durchführungsakte festlegelegt, die von der EU-Kommission erlassen werden. In der Durchführungsverordnung 2023/138 [3]hat die Kommission festgelegt, dass zu den hochwertigen Datensätzen etwa Daten zur Meteorologie, zur Erdbeobachtung und Umwelt und zur Mobilität zählen.

Die Weiterverwendung der Daten ist nicht auf bestimmte Zwecke beschränkt. Stattdessen normiert § 4 Abs. 1 DNG, dass Daten für jeden kommerziellen oder nichtkommerziellen Zweck genutzt werden können. Möglich ist jedoch, dass die öffentlichen Stellen die Weiterverwendung nur unter bestimmten Nutzungsbedingungen einräumen. Hierbei kann etwa vereinbart werden, dass die Daten nur weiterverwendet werden dürfen, wenn sie selbst nicht inhaltlich verändert werden. § 4 Abs. 3 DNG legt hierzu fest, dass Nutzungsbedingungen zulässig sind, sofern sie objektiv, verhältnismäßig, nichtdiskriminierend und durch ein im Allgemeininteresse liegendes Ziel gerechtfertigt sind. Nach Möglichkeit sollen offene Nutzungsbedingungen verwendet werden. Zum Ziel der uneingeschränkten Datennutzung trägt auch das Verbot der Ausschließlichkeitsvereinbarungen nach § 6 Abs. 1 DNG bei. Hiernach dürfen grundsätzlich keine ausschließlichen Rechte an der Nutzung von Daten gewährt werden. Dies gilt nicht, sofern eine ausschließliche Datennutzung zur Bereitstellung eines Dienstes im öffentlichen Interesse erforderlich ist (§ 6 Abs. 2 DNG). Im Grundsatz soll die Weiterverwendung der Daten unentgeltlich möglich sein. Gemäß § 10 Abs. 1 DNG dürfen in der Regel lediglich

3 Abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32023R0138 (zuletzt abgerufen am 05.12.2023).

Bearbeitungsgebühren verlangt werden, die den Aufwand decken. Bestimmte Einrichtungen dürfen jedoch in Abweichung hiervon weitere Entgelte verlangen. Gemäß § 10 Abs. 2 DNG zählen hierzu etwa Bibliotheken, Archive und öffentliche Stellen, die auf die Erzielung von Einnahmen angewiesen sind, um die Kosten für die Erfüllung öffentlicher Aufträge decken zu können.

3. Lediglich Regelung der Weiterverwendung, nicht des Zugangs

§ 1 Abs. 2 DNG legt ausdrücklich fest, dass das Gesetz keine Pflicht zur Bereitstellung und keinen Anspruch auf Zugang der Daten begründet. Da das DNG in seinem Anwendungsbereich allerdings voraussetzt, dass Daten bereits zugänglich gemacht wurden, wird § 1 Abs. 2 DNG so verstanden, dass aus dem DNG lediglich kein Anspruch auf Erst-Zugang folgt. Entscheidet sich eine Behörde jedoch Daten zugänglich zu machen, hat sie die Vorgaben des DNG zu beachten und darf insbesondere keine Ausschließlichkeitsvereinbarungen treffen. Aus der bisherigen Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) (Az. 7 C 12/14) folgt, dass ein Zugangsrecht zu Informationen besteht, sofern eine öffentliche Stelle diese Informationen bereits zuvor von sich aus veröffentlicht hat.

III. Der Data Governance Act

Das DNG hat unterschiedliche Kategorien von Daten aus seinem Anwendungsbereich ausgeschlossen, insbesondere solche, bei denen besondere Schutzrechte an den Daten bestehen. Kommt es zu einer (rechtmäßigen) Weiterverwendung solcher Daten, werden die Modalitäten hierfür im Data Governance Act (DGA) festgelegt. Die Regeln finden gemäß Art. 3 Abs. 1 DGA Anwendung auf Daten, die sich im Besitz öffentlicher Stellen befinden und aus Gründen der geschäftlichen Geheimhaltung (lit. a), der statistischen Geheimhaltung (lit. b), des Schutzes geistigen Eigentums Dritter (lit. c) oder des Schutzes personenbezogener Daten (lit. d) geschützt sind. Sofern sich die Daten im Besitz einer Bildungseinrichtung befinden, finden die Regeln gemäß Art. 3 Abs. 2 lit. c DGA jedoch keine Anwendung. Der DGA definiert Bildungseinrichtungen nicht selbst, jedoch ist davon auszugehen, dass Hochschulen hiervon umfasst sind und somit aus dem Anwendungsbereich des DGA ausgenommen sind.

Die Bestimmungen des DGA zur Weiterverwendung von Daten ähneln den Regelungen des DNG. Gemäß Art. 4 DSA sind Vereinbarungen, die ausschließliche Rechte an Daten gewähren, grundsätzlich verboten. Ausnahmen sind im allgemeinen Interesse möglich. Gemäß Art. 5 Abs. 3 DSA gilt auch hier, dass die Bedingungen für die Weiterverwendung von Daten nichtdiskriminierend, verhältnismäßig und objektiv gerechtfertigt sein müssen. Sie dürfen nicht der Behinderung des Wettbewerbs dienen. Die gleichen Anforderungen müssen gemäß Art. 6 Abs. 1 DGA auch etwaige Gebühren erfüllen, die von den öffentlichen Stellen für die Erlaubnis der Weiterverwendung erhoben werden.

IV. Relevanz für Hochschulen

Den Open-Data-Regelungen müssen auch von Hochschulen und anderen wissenschaftlichen Einrichtungen beachtet werden. Das DNG erwähnt ausdrücklich Forschungseinrichtungen und bestimmt für sie einen eigenen Anwendungsbereich. Sofern Forschungsdaten öffentlich finanziert wurden und über ein Archiv der Öffentlichkeit bereitgestellt wurden, sind die Vorschriften des DNG für die Weiterverwendung zu beachten. Die Daten müssen in möglichst offenen Formaten und unter nichtdiskriminierenden Bedingungen zu jeglichen Zwecken weiterverwendet werden können.

Gemeinsam sind wir verantwortlich!

Fehlende Vereinbarung bei gemeinsamer Verantwortung ist ein Bußgeldrisiko

von Marc-Philipp Geiselmann

Das Führen einer gemeinsamen Kundendatenbank durch mehrere Unternehmen ohne entsprechende Vereinbarung kann zu einem Bußgeld von 13.000 Euro führen, wenn die beteiligten Unternehmen keine Vereinbarung abschließen, die regelt, welches Unternehmen die diversen Pflichten der DSGVO erfüllt.

I. Hintergrund

Anlass dieses Schreibens ist eine Bußgeldforderung in Höhe von 13.000 Euro durch den Hamburgischen Datenschutzbeauftragten.[1] Was war passiert? Ein Unternehmen hatte einem Kunden die Buchung für einen Online-Kurs verweigert, da dieser noch Zahlungsrückstände bei einem anderen Unternehmen aufgrund eines anderen Online-Kurses hatte. Das Unternehmen wusste von den Rückständen, da beide Unternehmen eine gemeinsame Kundendatenbank führen. Der abgelehnte Kunde hat daraufhin eine Beschwerde beim Hamburgischen Datenschutzbeauftragen erhoben. Er war der Meinung, dass das gemeinsame Führen einer Kundendatenbank gemäß Art. 26 DSGVO zu einer gemeinsamen Verantwortlichkeit führt und deshalb eine schriftliche Vereinbarung erforderlich ist, die die Unternehmen jedoch nicht abgeschlossen hatten.

II. Das Rechtsinstitut der „gemeinsamen Verantwortung“

Für das Führen einer gemeinsamen Kundendatenbank durch zwei oder mehrere Unternehmen gibt es gute Gründe. Es ergeben sich dadurch Synergieeffekte für die Beteiligten. Zum einen kann der Aufwand für die Pflege der Datenbank unter den Unternehmen aufgeteilt werden und zum anderen besteht Schutz vor unredlichen Kunden, die bei anderen Unternehmen bereits säumig sind, wie im Beispiel oben genannt. Je nach Ausgestaltung der Organisation der gemeinsamen Kundendatenbank kann eine gemeinsame Verantwortung nach Art. 26 DSGVO vorliegen. Dieses Rechtsinstitut war in Deutschland bis zur Einführung der DSGVO weitgehend unbedeutend.[2] Seit der Einführung der DSGVO erlangte es auch durch die Rechtsprechung des EuGHs immer mehr an Bedeutung.[3] Es führte unter anderem dazu, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) dem Press- und Informationsamt der Bundesregierung den Betrieb der Facebook-Seite der Bundesregierung untersagte.[4]

1 29. Tätigkeitsbericht Datenschutz 2020 – HmbBfDI, S. 119.

2 https://www.lda.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf (zuletzt abgerufen am 15.12.2023).

3 Siehe die Urteile EuGH, Urteil vom 5.6.2018 – C-210/16 – ULD Schleswig-Holstein/Wirtschaftsakademie Schleswig-Holstein; dazu auch Baur, „Auch aus kleiner Kraft folgt große Verantwortung“ im DFN-Infobrief Recht 08/2018 und zur Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder: Baur, „So nicht, mein Facebook-Freund!“ im DFN-Infobrief Recht 06/2019; EuGH, Urteil vom 29.7.2019 – C-40/17 – Fashion ID; EuGH, Urteil vom 10.7.2018 – C-25/17 in EuGH ZD 2018, 469 m. Anm. Hoeren.

4 Rennert, „Ciao, Fanpages!“ im DFN-Infobrief Recht 04/2023.

Verantwortlicher ist die Person, die über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; das heißt, sie entscheidet über das „Ob“ und „Wie“ der Datenverarbeitung.[5]

Dies ist zu unterscheiden vom Auftragsverarbeiter, also der Person, an die die Datenverarbeitung ausgelagert wurde.[6] Der Auftragsverarbeiter ist kein „gemeinsamer“ Verantwortlicher, sondern nur diejenige Person, die die Datenverarbeitung im Auftrag des Verantwortlichen durchführt. Die beiden Akteure in der Datenverarbeitung unterscheiden sich darin, dass der Verantwortliche dem Auftragsverarbeiter gegenüber weisungsgebunden ist. Der Verantwortliche hat also eine Entscheidungsbefugnis über Zwecke und Mittel der Verarbeitung und ein Eigeninteresse an der Datenverarbeitung.

Eine gemeinsame Verantwortlichkeit setzt eine gemeinsame Festlegung der Zwecke und Mittel voraus. Die Art der Zusammenarbeit kann vielfältig gestaltet und muss nicht zwangsläufig gleichrangig sein. Der mit der Datenverarbeitung verfolgte Zweck kann ein gemeinsamer Zweck sein oder jeweils ein eigener Zweck, sofern die Zwecke gemeinsam verfolgt werden. In Anlehnung an das eingangs erwähnte Beispiel kann ein Verantwortlicher die Kundendatenbank zur Betrugsprävention und ein anderer Verantwortlicher sie für eine Rabattaktion nutzen.

Auch in zeitlicher Hinsicht muss sich die gemeinsame Verantwortlichkeit nicht vollständig decken. Eine gemeinsame Verantwortlichkeit während einzelner Phasen der Datenverarbeitung reicht aus. Zusätzlich zur gemeinsamen Festlegung der Zwecke ist auch eine gemeinsame Festlegung der Mittel der Datenverarbeitung erforderlich. Nur wenn beide Parteien sowohl über Zweck als auch Mittel entscheiden, kann von einer gemeinsamen Verantwortlichkeit gesprochen werden.
Eine gemeinsame Verantwortlichkeit ist nicht ausgeschlossen, wenn die Beteiligten die Zusammenarbeit als Auftragsverarbeitung bezeichnen. Maßgeblich sind die tatsächlichen Verhältnisse unabhängig von der Bezeichnung durch die Beteiligten.
Abschließend ist zu erwähnen, dass es kein „Konzernprivileg“ gibt. Sofern die Unternehmen rechtlich selbstständige juristische Personen sind, kommt eine gemeinsame Verantwortlichkeit in Betracht.

III. Rechtsfolgen einer gemeinsamen Verantwortung – Abschluss einer Vereinbarung

Liegt eine gemeinsame Verantwortlichkeit vor, so sieht Art. 26 Abs. 1 S. 2 DSGVO vor, dass eine Vereinbarung abgeschlossen werden muss.
In der Vereinbarung müssen die Verantwortlichen klar definieren, wer die allgemeinen Datenschutzgrundsätze erfüllt, für die Rechtmäßigkeit der Datenverarbeitung verantwortlich ist und die Informationspflichten nach Art. 13 f. DSGVO erfüllt sowie wer welche Sicherheitsmaßnahmen ergreift. Außerdem muss geregelt werden, wer der Meldepflicht nachkommt und die Datenschutz-Folgenabschätzung durchführt.[7] Die beteiligten Verantwortlichen haben hierbei flexibel die Möglichkeit, die Verantwortlichkeiten aufzuteilen. Es ist nicht erforderlich, dass jede Partei Aufgaben in gleichem Umfang wahrnimmt.

Die Vereinbarung allein stellt keine Grundlage für die Rechtmäßigkeit der Datenverarbeitung dar. Es muss für die Verarbeitung der Daten ein allgemeiner Rechtsgrund beispielsweise nach Art. 6 DSGVO vorliegen. Auch für die Übermittlung der Daten zwischen den gemeinsamen Verantwortlichen ist ein allgemeiner Rechtsgrund erforderlich. Ist dieser eine Einwilligung gem. Art. 6 Abs. 1lit. a DSGVO, so muss diese sich auch auf die Übermittlung beziehen.

Es gibt keine vorgeschriebene Form für die Vereinbarung. Jedoch empfiehlt sich die schriftliche oder elektronische Form, um der Transparenzpflicht nachzukommen. Die Vereinbarung muss wahrheitsgemäß sein und die tatsächlichen Gegebenheiten der Datenverarbeitung darstellen. Die verschiedenen Phasen der Datenverarbeitung sowie die jeweils verantwortliche Partei und das verwendete Programm sind zu benennen.

Eine Angabe einer Anlaufstelle für betroffene Personen ist jedoch freiwillig. Betroffene Personen müssen sich nicht an die Anlaufstelle wenden, sondern können gemäß Art. 26 Abs. 3 DSGVO ihre Rechte bei jedem Verantwortlichen geltend machen.

Den betroffenen Personen müssen die wesentlichen Informationen zur Verfügung gestellt werden. Wesentlich ist nicht

5 BeckOK DatenschutzR/Spoerr, DS-GVO Art. 26 Rn. 17.

6 Der Auftragsverarbeiter ist in Art. 28 DSGVO geregelt.

7 Gola/Heckmann/Piltz, DS-GVO Art. 26 Rn. 23.

die komplette Vereinbarung, sondern nur die Informationen, die für die betroffene Person relevant sind, um ihre Rechte nach der DSGVO geltend zu machen. Dazu zählen die an der Datenverarbeitung beteiligten Verantwortlichen, die mit der Datenverarbeitung verfolgten Ziele, die verarbeiteten Daten sowie die Verantwortlichkeit für die Informationspflichten[8]. Außerdem ist relevant, wie die Verantwortlichen zusammenwirken. Wie diese Informationen bereitgestellt werden, ob auf einer öffentlich zugänglichen Webseite oder auf Anfrage, wird von der Verordnung nicht näher festgelegt.

So soll Art. 26 DSGVO sicherstellen, dass ein Verantwortlicher seiner datenschutzrechtlichen Verantwortung nicht entgeht, wenn er Daten gemeinsam mit einem anderen Verantwortlichen verarbeitet und Kontrolle über die Zwecke und Mittel der Verarbeitung hat. Art 26 DSGVO soll auch verhindern, dass eine betroffene Person seine datenschutzrechtlichen Rechte nicht geltend macht, weil sie durch die unterschiedlichen Verantwortlichkeiten verunsichert ist. Es werden Anforderungen an die Transparenz und die Rechtmäßigkeit der Datenverarbeitung gestellt.

Der Abschluss einer Vereinbarung ist nicht konstitutiv für das Vorliegen einer gemeinsamen Verantwortlichkeit. Maßgeblich sind die oben dargelegten Kriterien.
Fehlt eine derartige Vereinbarung, so kann dies gemäß Art. 83 Abs. 4 lit. a DSGVO mit einer Geldbuße sanktioniert werden. Diese kann bis zu 10 Millionen Euro oder, bei Unternehmen, bis zu 2 % des weltweiten Jahresumsatzes betragen.

IV. Fazit und Hochschulbezug

Die Verpflichtung zum Abschluss einer solchen Vereinbarung sollte bekannt sein und muss befolgt werden. Bevor ein solcher Vertrag abgeschlossen wird, sollte zuerst sorgfältig geprüft werden, ob eine gemeinsame Verantwortlichkeit besteht. Ist dies der Fall, sollten die Gründe dafür dokumentiert werden, da diese Einschätzung auch falsch sein kann. Der Abschluss eines solchen Vertrags ist jedoch keine schwierige Aufgabe, sondern zwingt die Verantwortlichen dazu, sich über die datenschutzrechtlichen Pflichten jedes Beteiligten im Klaren zu sein. Die Regelungen gelten auch für Hochschulen. Gemeinsame Datenbanken von verschiedenen Hochschulen, Studierendenwerken oder Unternehmen wären denkbar. Dies kann innerhalb einer kontinuierlichen Zusammenarbeit oder zeitlich begrenzter (Forschungs-) Projekte geschehen.

Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg hat einen Entwurf für eine Vereinbarung bereitgestellt, der zum Download verfügbar ist.
(Stand: Dezember 2023): https://www.baden-wuerttemberg.datenschutz.de/mehr-licht-gemeinsame-verantwortlichkeit-sinnvoll-gestalten/

V. Ausblick

Auch für neue Technologien beansprucht Art. 26 DSGVO Geltung. Die arbeitsteilige Entwicklung von KI-Systemen kann auch eine gemeinsame Verantwortlichkeit begründen. Diese Ansicht wird in der Literatur vertreten bei abgesprochenen Anpassungen des KI-Systems mit dem Anbieter.[9] Des Weiteren sieht der Entwurf der EU-Kommission zum AI-Act einen Übergang der Anbieterpflichten in Art. 28 AI-Act-E[10] vor. Das Rechtsinstitut der gemeinsamen Verantwortlichkeit wird in Zukunft wohl noch weiter an Bedeutung gewinnen. Auch dies sollten Hochschulen bei gemeinsamen Forschungsprojekten beachten.

8 BeckOK DatenschutzR/Spoerr, DS-GVO Art. 26 Rn. 57.

9 Hacker/Berz, Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, ZRP 2023 226 (228).

10 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa-75ed71a1.0019.02/DOC_1&format=PDF (zuletzt abgerufen am 11.12.2023).

Bist du ein personenbezogenes Datum?

Die Trilogie der europäischen Rechtsprechung zum Personenbezug von Daten

Von Ole-Christian Tech

Die wohl grundlegendste Frage des Datenschutzrechts ist zugleich auch eine der umstrittensten. Die Frage, ab wann Daten überhaupt personenbezogen sind, ist die Kardinalfrage des gesamten Datenrechts. Von ihr hängt der grundrechtliche Schutzbereich nach Art. 8 der europäischen Grundrechtecharter (GRCh), die Anwendung der Datenschutzgrundverordnung (DSGVO) und des nationalen Datenschutzrechts – mit all seinen Anforderungen und Haftungsrisiken – sowie die Abgrenzung zu anderen Rechtsakten, wie etwa der „Free Flow of Data"-Verordnung, ab.[1] Die Trilogie der europäischen Rechtsprechung hierzu ist daher einen vertieften Blick wert.

I. Einordnung

Personenbezogen sind Daten nach Art. 4 Nr. 1 DSGVO dann, wenn diese einer bestimmten Person zugeordnet werden können. Dies erfasst einerseits den Fall, dass die Identität einer Person unmittelbar aus der Information selbst folgt. Andererseits aber auch den Fall, dass Verknüpfungen mit weiteren Informationen die Person direkt oder indirekt identifizierbar, also **bestimmbar** machen. Ein Datum ist jedenfalls dann personenbezogen, wenn der Verantwortliche selbst, dieses einer natürlichen Person eindeutig zuordnen kann.
Bei der Auslegung des Begriffs „bestimmbar" unterscheidet man in der Literatur und Praxis zwischen einem absoluten und einem relativen Verständnis des Personenbezugs.

Der absolute Ansatz (auch objektiver Ansatz genannt):

Nach dem absoluten Ansatz sind Daten dann personenbezogen, wenn eine Person auch nur theoretisch identifiziert werden kann. Somit reicht es aus, wenn auch nur hypothetisch durch einen weiteren Verarbeitungsschritt oder etwaiges Zusatzwissen (auch dritter Personen) ermöglicht wird, einen Bezug zwischen der Information und der betroffenen Person herzustellen.[2] In der Konsequenz führt dieser Ansatz regelmäßig zum Vorliegen personenbezogener Daten und weitet somit den Anwendungsbereich der DSGVO erheblich aus.[3] Somit überrascht es kaum, dass dieser Ansatz besonders von Datenschutzaufsichtsbehörden vertreten wird,[4] die hierdurch letztlich auch ihren Kompetenzbereich erweitern.

Der relative Ansatz (auch subjektiver Ansatz genannt):

Der relative Ansatz erkennt Daten erst dann als personenbezogen an, wenn diese vom Verantwortlichen tatsächlich im konkreten Fall einer Person zugeordnet werden können. Relevant ist also nur das Zusatzwissen des Verantwortlichen bzw. seine technischen oder rechtlichen Möglichkeiten, dieses zu gewinnen.[5] Konsequenz aus diesem Ansatz ist, dass nicht immer zu

1 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32018R1807 (zuletzt abgerufen am 08.12.2023).

2 Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art.4 Rn. 57.

3 Brink/Eckhardt ZD 2015, 205 (206).

4 Karg in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art. 4 DSGVO Rn.58; Klar/Kühling in: Kühling/Buchner, DSGVO 4. Auflage 2024, Art. 4 Nr. 1 Rn. 25 m.W.N.

5 Brink/Eckhardt ZD 2015, 205 (206); Karg in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 1. Auflage 2019, Art.4 Rn. 59.

jedem Zeitpunkt bestimmt werden kann, ob verarbeitete Daten Personenbezug haben oder nicht. Dieser Ansatz ist durchaus „industriefreundlicher“ und wird daher überwiegend in der Praxis vertreten.[6] Diese Auffassung kann als herrschend in der datenschutzrechtlichen Literatur betrachtet werden.

Die bis heute grundlegendste Rechtsprechung des Europäischen Gerichtshofs (EuGH) hierzu in der Rechtssache Breyer ist noch unter der Richtlinie 95/46/EG, also der Datenschutzrichtlinie ergangen, aber aufgrund der identischen Terminologie und Regelungssystematik auch unter der inzwischen in Kraft getretenen DSGVO gültig.

Die Festlegung auf die Bestimmbarkeit folgt bereits aus Art. 8 Abs. 1 GRCh: „Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.“ Diese Formulierung erklärt im Übrigen auch den Fokus des geltenden Datenrechts auf die Einordnung personenbezogener Daten als Schutzgut (Vgl. Art. 1 Abs.1 und 2 DSGVO), im Gegensatz zu einem Wirtschaftsgut, dessen ökonomisches Potenzial es zu erschließen gilt. Gleichwohl hat auch der Unionsgesetzgeber in Art. 1 Abs. 3 DSGVO den freien Verkehr personenbezogener Daten in der Union als Ziel benannt. Diese Entscheidung muss somit auch bei der Auslegung der unbestimmten Rechtsbegriffe im Datenschutzrecht berücksichtigt werden, sodass es verfehlt wäre, anzunehmen, Datenschutz sei der alleinige oder gar ein Selbstzweck der DSGVO.

Die Begriffe „Daten“, „Informationen“ und „Wissen“ werden in der juristischen Literatur nicht immer einheitlich verwendet und selbst die Legaldefinitionen unterscheiden sich von Gesetz zu Gesetz mitunter erheblich. Während Daten in der DSGVO gar nicht definiert werden, sondern lediglich als personenbezogene Daten auftauchen (Art. 4 Nr. 1 DSGVO), enthalten andere Rechtsakte durchaus eine Begriffsbestimmung, wie etwa in Art. 2 Nr. 1 des Data Governance Acts (DGA): *„Daten“ [sind] jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“*.

Für ein grundlegendes Verständnis sollte jedoch folgendes Schaubild förderlich sein, welches die Begriffe einem Verarbeitungsgrad zuordnet.

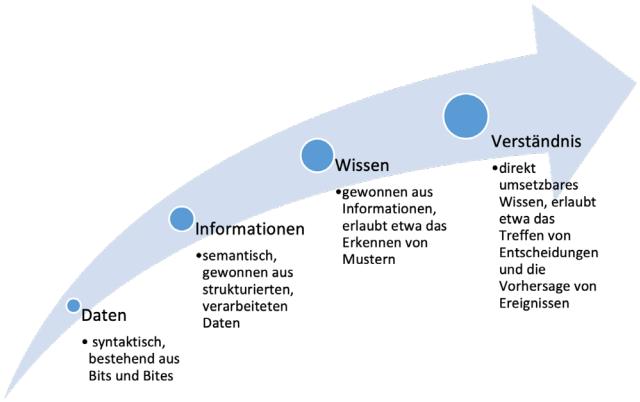

Abbildung: Datenzyklus

II. Breyer

1. EuGH Urteil vom 19.10.2016, C-582/14

Herr Breyer besuchte unterschiedliche Websites von Bundesbehörden, auf denen aktuelle Informationen veröffentlicht werden. Um Angriffe zu vermeiden und Straftäter zu verfolgen, werden auf den meisten dieser Websites sämtliche Zugriffe in Protokolldateien aufgezeichnet. Diese beinhalten den Namen der aufgerufenen Seite oder Datei, die in Suchfeldern eingegebenen Begriffe sowie den Zeitpunkt des Abrufs.

Im Falle eines Abrufs werden die übertragene Datenmenge, der Status des Abrufs sowie die IP-Adresse des zugreifenden Rechners gespeichert. Um die abgerufenen Daten an den korrekten Empfänger übermitteln zu können, wird beim Zugriff auf eine Website die IP-Adresse des Abrufenden an den Server übermittelt, auf dem sich die angeforderte Website befindet.

Herr Breyer klagte und beantragte, dass die Bundesrepublik Deutschland die IP-Adresse seines zugreifenden Hostsystems nicht länger über das Ende des Zugriffs auf allgemein zugänglichen Websites für Online-Mediendienste der Einrichtungen des Bundes hinaus speichern oder durch Dritte speichern lässt, es sei denn, die Speicherung ist im Störungsfall zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich. Das erstinstanzliche Gericht (Amtsgericht (AG) Tiergarten) hatte die Klage abgewiesen. Daraufhin legte der Kläger Berufung ein. Im Berufungsverfahren hat das Landgericht (LG) Berlin die

6 Ziebarth in: Sydow/Marsch, DS-GVO, 3. Auflage 2022, Art. 4 Rn. 35ff; Schulz in: Gola/Heckmann, DSGVO, 3. Auflage 2022 Art. 4 DSGVO Rn. 21.

Entscheidung des erstinstanzlichen Gerichts teilweise abgeändert. Die Bundesrepublik Deutschland wurde zur Unterlassung der Speicherung der IP-Adresse des zugreifenden Hostsystems von Herrn Breyer verurteilt, welche im Zusammenhang mit seinem Zugriff auf öffentlich zugängliche Websites für Online-Mediendienste der Einrichtungen des Bundes übertragen wird. Die Speicherung über das Ende des jeweiligen Nutzungsvorgangs hinaus oder durch Dritte ist nicht gestattet. Sofern Herr Breyer während des Zugriffs seine Personalien einschließlich einer E-Mail-Adresse zur Identifikation angegeben hat, kann die Adresse in Verbindung mit dem Zeitpunkt des Zugriffs für eine begrenzte Zeit gespeichert werden. Eine Speicherung ist nur im Fall von Störungen zur Wiederherstellung der Verfügbarkeit des Telemediums erforderlich.

Sowohl Herr Breyer als auch die Bundesrepublik Deutschland haben Revision beim Bundesgerichtshof (BGH) gegen die Entscheidung des Berufungsgerichts eingelegt.
Unter diesen Umständen hat der BGH beschlossen, das Verfahren auszusetzen und dem EuGH (unter anderem) folgende Frage zur Vorabentscheidung vorzulegen:
Ist Art. 2 Buchst. a der Richtlinie 95/46 dahin auszulegen, dass eine IP-Adresse, die ein Anbieter von Online-Mediendiensten im Zusammenhang mit einem Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (hier: Zugangsanbieter) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt?

Exkurs IP Adressen:
Eine IP-Adresse (Internet Protocol Address) ist wie eine Hausnummer für Computer im Internet. Sie identifiziert einen Computer oder ein Gerät eindeutig im Netzwerk.

Es gibt dabei zwei Haupttypen von IP-Adressen: IPv4 (zum Beispiel: 192.168.1.1) und IPv6 (zum Beispiel: 2001:0db8:85a3:0000:0000:8a2e:0370:7334).

IP-Adressen können entweder statisch oder dynamisch sein.

Eine dynamische IP-Adresse kann sich ändern. Wenn ein Gerät eine Verbindung zum Internet herstellt, weist der Internetdienstanbieter (ISP, Internet Service Provider) ihm vorübergehend eine IP-Adresse zu. Bei jeder neuen Verbindung kann dem Gerät eine andere IP-Adresse zugewiesen werden.
Dynamische IP-Adressen werden normalerweise von Internetdienstanbietern dynamisch zugewiesen und können sich im Laufe der Zeit ändern. Im Gegensatz dazu bleibt eine statische IP-Adresse unverändert und wird normalerweise manuell konfiguriert.

2. Das Urteil des EuGHs

Der EuGH erinnert zunächst an seine bisherige Rechtsprechung zum Personenbezug von IP-Adressen in der Rechtssache Scarlet Extended (EuGH Urteil vom 24. November 2011 C-70/10), in welcher das Gericht zu der Erkenntnis gelangte, dass IP-Adressen geschützte personenbezogene Daten sind, da sie die genaue Identifizierung der Nutzer ermöglichen.[7]

Jedoch hatte im damaligen Fall der Internetzugangsanbieter die Sammlung und Identifizierung der IP-Adressen der Internetnutzer selbst vorgenommen.[8] Somit hatte der Verantwortliche das entsprechende Zusatzwissen zur Identifizierung selbst inne.
Im vorliegenden Fall hat die Bundesrepublik zwar die IP-Adressen der Webseitenbesucher, aber eben nicht die Provider-Daten. Erst mit diesem Abgleich könnte eine Identifizierung des Betroffenen gelingen.[9] Das hierfür erforderliche Zusatzwissen hat nur der jeweilige Internetzugangsanbieter (Provider).

Für die Beantwortung der Frage, ob eine Person identifizierbar ist, sind **alle Mittel** zu berücksichtigen, die **vernünftigerweise** entweder von dem **Verantwortlichen** für die Verarbeitung **oder** von einem **Dritten**[10] eingesetzt werden könnten.[11] Demnach ist es für einen Personenbezug nicht notwendig, dass Daten und Zusatzwissen bei derselben Person zeitgleich vorliegen.

7 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 33; EuGH Urteil vom 24. November 2011 C-70/10 Rz. 51.

8 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 34.

9 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 37.

10 Hervorhebungen durch den Autor.

11 So etwa Erwägungsgrund 26 der Datenschutzrichtlinie, inhaltlich genauso auch Erwägungsgrund 26 der DSGVO.

Somit musste der EuGH also die Frage beantworten, ob bereits die bloße Möglichkeit, eine (noch dazu dynamische) IP-Adresse mit den Providerdaten zu verknüpfen, ein „Mittel“ ist, dass vernünftigerweise zur Bestimmung der betreffenden Person eingesetzt werden kann.[12]

Das Gericht definiert hierbei nicht konkret, wie diese Mittel, die vernünftigerweise eingesetzt werden können, zu bestimmen sind. Sie lägen jedoch jedenfalls dann nicht vor, wenn „die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde, sodass das Risiko einer Identifizierung de facto vernachlässigbar erschiene.“[13]

Das deutsche Recht kennt zwar keine generelle Anspruchsgrundlage für die Herausgabe von Zusatzinformationen gegenüber Internetprovidern, aber sehr wohl eine Reihe von Spezialgesetzen, die es etwa im Fall von Cyberattacken ermöglichen, diese Daten mithilfe von Behörden zu erlangen und z.B. eine Strafverfolgung zu ermöglichen.[14] Im deutschen Recht besteht diese Möglichkeit etwa mit § 100g Strafprozessordnung (StPO) i.V.m. § 406e StPO. Hiernach kann die Staatsanwaltschaft als Ermittlungsbehörde nach § 100g StPO zur Ermittlung entsprechende personenbezogene Daten als Verkehrsdaten erheben, die dann nach § 400e StPO im Wege der Akteneinsicht auch der verletzten Person zugänglich gemacht werden. Weitere denkbare Anspruchsgrundlagen bestehen etwa in § 101 Urheberrechtsgesetz (UrhG) oder §§ 1 Abs. 1 Satz 1 Informationsfreiheitsgesetz (IFG).
Diese durchaus begrenzte Möglichkeit reicht nach Auffassung des EuGHs bereits als rechtliches Mittel, das vernünftigerweise Weise eingesetzt werden könnte, um die natürliche Person zu identifizieren. Damit stellen IP-Adressen personenbezogene Daten dar.[15]

Diese Erkenntnis des Gerichts ist durchaus bemerkenswert, da der BGH in seinem Vorlagebeschluss an den EuGH noch explizit hervorgehoben hat, dass der Webseitenbetreiber im konkreten Fall keinen Auskunftsanspruch gegen den Provider hatte.[16] Die Auslegung des EuGHs ist somit eine äußerst extensive, womit auch der sachliche Anwendungsbereich der DSGVO stark erweitert wird.

Insgesamt positioniert sich der EuGH mit dem Urteil in der Rechtssache Breyer also in der Tendenz zugunsten eines modifizierten relativen Ansatzes, da es für einen Personenbezug auf die tatsächliche oder rechtliche Möglichkeit ankommt, die Person (auch mittels noch zu erlangenden Zusatzwissens) zu identifizieren. Eine klare Absage an den absoluten Ansatz hat der Gerichtshof jedoch auch nicht erteilt. Schließlich sind die rechtlichen und tatsächlichen Möglichkeiten im zugrundeliegenden Urteil derart weit gefasst worden, dass in der Konsequenz der Anwendungsbereich der DSGVO eher dem unter dem absoluten Ansatz ähnelt. Der in der Rechtssache Breyer dargestellte Ansatz lässt sich daher eher als Kompromiss verstehen, der jedoch weniger Rechtssicherheit für die Praxis bringt, als allgemein erwartet wird.

III. SRB gegen EDSB

1. EuG Urteil vom 26.04.2023, T-557/20

Der Single Resolution Board (SRB) ist eine EU-Institution, die die ordnungsgemäße Abwicklung von insolvenzbedrohten Finanzinstituten sicherstellen soll. Hierfür nutzte der SRB im Rahmen des Abwicklungsverfahrens gegen die Banco Popular Español ein elektronisches Formular, mit dem Anteilseigner und Gläubiger Stellung nehmen konnten. Die eingegangenen Antworten wurden an das Beratungsunternehmen Deloitte als unabhängigen Gutachter weitergeleitet, um so relevante Stellungnahmen auswerten zu lassen. Bevor die Antworten weitergegeben wurden, ersetzte der SRB den Namen jedes Befragten durch einen Code.

12 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 45.

13 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 46; aufgrund des Ausschlusses gesetzlich verbotener Mittel ist diese Rechtsprechung zugleich eine Absage an die in Teilen der Literatur vertretene Auffassung, auch illegale Mittel seien bei den Identifizierungsmöglichkeiten zu berücksichtigen, z.B. Bergt ZD 2015, 365 (370).

14 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 47.

15 EuGH Urteil vom 19.10.2016, C-582/14 Rz. 49.

16 BGH Beschluss vom 28.10.2014 – VI ZR 135/13 Rz. 32.

Nach einer Reihe von Beschwerden entschied der Europäische Datenschutzausschuss (EDSB), dass die pseudonymisierten Daten, die vom SRB weitergegeben wurden, personenbezogen waren. Der Code, mit dem die Antworten aus der Registrierungsphase und der Konsultationsphase verknüpft wurden, wurde ebenfalls geteilt, ohne dass das Beratungsunternehmen während der Registrierungsphase Identifikationsdaten von den Teilnehmern erhalten hatte.
Die Antworten seien laut EDSB als personenbezogene Daten anzusehen. Die Nichtnennung des Beratungsunternehmens als potenzieller Empfänger personenbezogener Daten in der Datenschutzerklärung des SRB wurde vom EDSB daher als Verstoß gegen die Informationspflichten gemäß Art. 15 Abs. 1 lit. d Verordnung 2018/1725 (Pendant Art. 13 Abs. 1 DSGVO) über Empfänger personenbezogener Daten betrachtet.

Der SRB war der Meinung, dass die Information über das Beratungsunternehmen als Empfänger personenbezogener Daten nicht erforderlich war. Die übermittelten Daten seien durch die Mitteilung des Codes nicht pseudonymisiert, sondern anonym. Sie konnten daher nicht als personenbezogene Daten für den Datenempfänger betrachtet werden. Eine Rückidentifizierung der Personen, die Stellungnahmen abgegeben haben, war anhand der den einzelnen Stellungnahmen zugewiesenen Codes technisch nicht möglich. Die in Artikel 3 Nummer 6 Verordnung 2018/1725 (übereinstimmend mit Artikel 4 Nummer 5 DSGVO) erwähnten zusätzlichen Informationen bestehen aus einer nur dem SRB zugänglichen Datenbank, die die Entschlüsselung ermöglicht. Es sei dem Beratungsunternehmen außerdem nicht gestattet gewesen, auf die zusätzlichen Informationen zuzugreifen, die eine Identifizierung ermöglicht hätten, sodass eine Rückidentifizierung der Personen auch rechtlich unmöglich sei.

2. Das Urteil des EuGs

Das Urteil des Europäischen Gerichts (EuG) in der Rechtssache SRB gegen EDSB betraf die Auslegung des Begriffs der personenbezogenen Daten nach der Verordnung (EU) 2018/1725. Diese stellt das Pendant zur DSGVO für Organe, Einrichtungen und sonstige Stellen der Europäischen Union dar, somit sind die entsprechenden Begriffsbestimmungen gleichlautend.

Exkurs zum EuG:

Der Gerichtshof der Europäischen Union besteht grundsätzlich aus zwei Instanzen, dem Gericht (früher: Gericht erster Instanz) und dem Gerichtshof (früher: Europäischer Gerichtshof).

Das EuG ist der Spruchkörper erster Instanz für verschiedene Verfahrensarten. Seine Aufgabe besteht darin, den EuGH zu entlasten, da dieser mit fortschreitender Harmonisierung des europäischen Rechts zunehmend ausgelastet war. Das EuG ist daher vor allem eine Tatsacheninstanz. Das Gericht besteht ab dem 1. September 2019 aus je zwei Richtern pro Mitgliedstaat. Diese werden von den Regierungen der Mitgliedstaaten im gegenseitigen Einvernehmen nach Anhörung eines Ausschusses für eine Amtszeit von 6 Jahren ernannt. Das EuG entscheidet in der Regel als Kammer oder in besonderen Fällen im Plenum, selten auch als Einzelrichter. Das EuG ist gemäß Art. 256 Abs. 1 AEUV und Art. 51 EuGH-Satzung insbesondere grundsätzlich zuständig für

- Nichtigkeitsklagen (Art. 263 AEUV)
- Untätigkeitsklagen (Art. 265 AEUV) und
- Schadensersatzklagen gegen die Union (Art. 268 AEUV).[17]

Der EuGH ist das oberste Gericht der Union und hat eine sogenannte Verwerfungskompetenz für Normen des Unionsrechts und kann Unionsrecht also für rechtswidrig erklären. Das Gericht entscheidet als Kammer, als Große Kammer oder in besonderen Fällen im Plenum. Es ist dabei grundsätzlich im zweiten Rechtszug sowie immer dann zuständig, wenn sich aus den Verträgen und der Satzung des EuGHs keine Zuständigkeit des EuGs ergibt. Der EuGH ist insbesondere zuständig im zweiten Rechtszug für Verfahren, die zuvor vor dem EuG verhandelt wurden (Art. 256 Abs. 1 UA 2 AEUV und Art. 56 ff. EuGH-Satzung), für Vertragsverletzungsverfahren (Art. 258-260 AEUV) und Vorabentscheidungsverfahren (Art. 267 AEUV).[18]

Das Gericht stellt vorab klar, dass die übermittelten Daten keine bereits identifizierten Personen betreffen.[19] Somit ist die im Urteil zu klärende Rechtsfrage erneut, ob die an Deloitte übermittelten Daten identifizierbare Personen betreffen. Das heißt, das Unternehmen müsste unter Berücksichtigung aller nach allgemeinem Ermessen wahrscheinlich nutzbarer Mittel einen Personenbezug aus diesen Daten herstellen können.

17 Zur Vertiefung siehe https://curia.europa.eu/jcms/jcms/J02_7033/de/ (zuletzt abgerufen am 08.12.2023).

18 Zur Vertiefung siehe https://curia.europa.eu/jcms/jcms/J02_7024/de/. (zuletzt abgerufen am 08.12.202).

19 EuG Urteil vom 26.04.2023, T-557/20 Rz. 84.

Anschließend rekurriert das Gericht auf die Rechtsprechung des EuGHs in der Rechtssache Breyer.[20] Hiernach besteht das Risiko einer Reidentifizierung dann nicht, wenn die Identifizierung der betreffenden Person gesetzlich verboten oder praktisch nicht durchführbar gewesen wäre, z. B. weil sie einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordert hätte, sodass das Risiko einer Identifizierung de facto als vernachlässigbar erschienen wäre.[21]

Im Fall der SRB hatte Deloitte lediglich den alphanumerischen Code erhalten, mit dem sie selbst die Verfasser nicht identifizieren konnten. Das für eine Identifizierung erforderliche Zusatzwissen befand sich ausschließlich in der Identifizierungsdatenbank der SRB.[22]

Nach der Lehre vom absoluten Personenbezug würde dies nun bereits ausreichen, um einen Personenbezug anzunehmen, da irgendjemand (hier die SRB) in der Lage ist, die Person zu identifizieren.

Diesem Ansatz folgt das EuG jedoch nicht. Vielmehr kommt es für die Bestimmung des Personenbezugs auf das Verständnis des Empfängers, also von Deloitte an. Nur wenn diese in der Lage ist, die Personen zu identifizieren, handelt es sich um personenbezogene Daten.[23]

Dabei hebt das Gericht zwei Aspekte hervor:

1. Zum einen hat auch der EDSB den Verstoß gegen die Informationspflicht nach Art. 15 Abs. 1 Buchst. d der Verordnung 2018/1725 mit der Übermittlung der Stellungnahmen mit dem alphanumerischen Code durch den SRB an Deloitte begründet und gerade nicht mit der Tatsache, dass der SRB über diese Informationen verfügte.[24]
2. Zum anderen vergleicht das Gericht den Sachverhalt mit der Situation in der Rechtssache Breyer. Deloitte sei wie der Online-Mediendienst, die Identifizierungsdatenbank und der SRB der Internetzugangsanbieter.[25] Somit hat nur der SRB die tatsächliche Möglichkeit der Identifizierung. Anders als in der Rechtssache Breyer bestehen hierbei aber keine – auch keine hypothetischen – Rechtsgrundlagen, aufgrund derer Deloitte eine rechtliche Möglichkeit der Identifizierung hätte.

Der EDSB hatte sich in seiner Entscheidung noch auf eine Prüfung der möglichen Rückidentifizierung aus der Perspektive des SRB beschränkt und somit die Lehre vom absoluten Personenbezug angewendet. Dem hat das EuG nun eindeutig eine Absage erteilt. [26]Nach der Prüfung des Gerichts unter Zugrundelegung des relativen Ansatzes aus der Rechtssache Breyer besteht ein solcher Personenbezug jedoch nicht.

Die Ausführungen des EuGs reichen weit über eine bloße Anwendung der Grundsätze aus der Breyer Rechtsprechung hinaus. Einerseits, weil sie die Lehre vom relativen Personenbezug bestätigen und andererseits, weil sie daraus unmittelbare Konsequenzen ableiten.

Wenn die Bekanntgabe pseudonymisierter Daten, d.h. solcher Daten bei denen der Empfänger keinen Personenbezug herstellen kann, keine Bekanntgabe personenbezogener Daten ist, dann hat dies erhebliche Auswirkungen auf die datenschutzrechtliche Praxis und die wirtschaftliche Nutzbarkeit von Daten.

So entfällt z. B. die Informationspflicht gegenüber dem Betroffenen. Der Auslandstransfer in Drittländer (wie zu Clouddienstleistern in den USA) ist unproblematischer, da weder Standardklauseln zu vereinbaren sind noch ein Transfer Impact Assessment durchzuführen ist.[27] Auch ein Dienstleister, der im Auftrag pseudonymisierte Daten verarbeitet und mit dem Auftragsdatenverarbeitungsvereinbarungen (ADVs) geschlossen werden müssen, ist kein Auftragsverarbeiter mehr.[28]

---

20 EuG Urteil vom 26.04.2023, T-557/20 Rz. 88.

21 EuG Urteil vom 26.04.2023, T-557/20 Rz. 93 mit Verweis auf EuGH Urteil vom 19. Oktober 2016, Breyer, C-582/14, Rz. 46.

22 EuG Urteil vom 26.04.2023, T-557/20 Rz. 94, 95.

23 EuG Urteil vom 26.04.2023, T-557/20 Rz. 97.

24 EuG Urteil vom 26.04.2023, T-557/20 Rz. 98.

25 EuG Urteil vom 26.04.2023, T-557/20 Rz. 99.

26 EuG Urteil vom 26.04.2023, T-557/20 Rz. 101-103.

27 Näheres zum Datentransfer bei Rüpke/ v. Lewinski/ Eckhardt: Datenschutzrecht, 2. Auflage München, 2022, S. 132ff.

28 Näheres zum Auftragsverarbeiter bei Rüpke/ v. Lewinski/ Eckhardt: Datenschutzrecht, 2. Auflage München, 2022, S. 154ff.

IV. Gesamtverband Autoteile-Handel e. V.

1. EuGH Urteil vom 09. November 2023, C 319/22

Scania, einer der größten Lkw-Hersteller in Europa, bietet über eine Website unabhängigen Wirtschaftsakteuren manuellen Zugang zu Fahrzeuginformationen, Informationen bezüglich der Reparatur und Wartung der Fahrzeuge sowie zu OBD-Informationen (On-Board-Diagnose-Informationen). Auf dieser Website ist es möglich, anhand von allgemeinen Fahrzeuginformationen wie Modell, Motorisierung oder Baujahr eine Suche durchzuführen oder gezielt nach einem bestimmten Fahrzeug anhand der sieben letzten Ziffern der Fahrzeugidentifizierungsnummer (kurz: FIN) zu suchen. Die Ergebnisse können lediglich als ausgedruckte Version oder als PDF-Datei auf dem Computer gespeichert werden, was einer automatisierten Datenverarbeitung entgegenwirkt. Ersatzteilinformationssuchergebnisse können als XML-Datei gespeichert werden.

Scania stellt diese Informationen unabhängigen Wirtschaftsakteuren nicht zur Verfügung. Zugriff auf diese Daten haben nur Werkstätten, entweder über die Zulassungspapiere oder durch die Angabe auf dem Fahrgestell des Kundenfahrzeugs, das zur Wartung oder Reparatur ansteht.

Der Gesamtverband Autoteile-Handel e. V. repräsentiert in Deutschland 80 Prozent des Umsatzes. Nach Einschätzung des Verbands genügt der von Scania gewährte Zugang zu den Informationen nicht den Anforderungen von Art. 61 Abs. 1 und 2 der Verordnung 2018/858 (ein sektorales Spezialgesetz über Kfz-Genehmigungen). Deshalb hat er beim Landgericht Köln beantragt, dass Scania verurteilt werden soll, den unabhängigen Wirtschaftsakteuren, die nicht als Reparaturbetriebe tätig sind, einen Zugang zu Reparatur- und Wartungsinformationen gemäß der Verordnung über eine Datenbankschnittstelle anzubieten, sodass maschinengesteuerte Suchanfragen gestellt und die Ergebnisse als Datensätze in einem für die Weiterverarbeitung bestimmten Format heruntergeladen werden können.
Das Vorlagegericht ist außerdem der Auffassung, dass die Fahrzeugidentifikationsnummer (FIN) in der Regel keine personenbezogenen Daten enthält. Dennoch stelle sich die Frage, ob Art. 61 der Verordnung 2018/858 so auszulegen ist, dass dieser für Fahrzeughersteller eine rechtliche Verpflichtung zur Verarbeitung von Daten gemäß Art. 6 Abs. 1 lit. c darstellt.
Unter diesen Umständen hat das LG Köln beschlossen, das Verfahren auszusetzen und dem EuGH (unter anderem) folgende Frage zur Vorabentscheidung vorzulegen:
Stellt Art. 61 Abs. 1 der Verordnung 2018/858 für Fahrzeughersteller eine rechtliche Verpflichtung im Sinne von Art. 6 Abs. 1 Buchst. c DSGVO dar, die die Herausgabe von FIN bzw. mit FIN verknüpften Informationen an unabhängige Wirtschaftsakteure als andere Verantwortliche im Sinne von Art. 4 Nr. 7 DSGVO rechtfertigt?

2. Das Urteil des EuGHs

Für die Beantwortung der Vorlagefrage ist entscheidend, ob es sich bei der FIN um personenbezogene Daten handelt, da anderenfalls der Anwendungsbereich der DSGVO nicht eröffnet und eine Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO nicht notwendig wäre.

Der EuGH stellt zu Beginn klar, dass Daten wie die FIN, ein alphanumerischer Code, den der Hersteller einem Fahrzeug zu dem Zweck zuweist, dass es einwandfrei identifiziert werden kann, für sich genommen noch keine „personenbezogenen“ Daten darstellen. Diese sind auf das jeweilige Fahrzeug bezogen und dienen der Identifizierung des Herstellers. Sie werden jedoch für denjenigen, der bei vernünftiger Betrachtung über Mittel verfügt, die es ermöglichen, sie einer bestimmten Person zuzuordnen, zu personenbezogenen Daten.[29]

Gemäß Anhang I Abschnitt II.5 der Richtlinie 1999/37 muss die Kfz-Zulassungsbescheinigung die FIN, den Namen und die Anschrift des Inhabers der Zulassungsbescheinigung enthalten.[30] Sofern der Halter oder eine als verfügungsberechtigt eingetragene Person eine natürliche Person ist, könnte es sich bei der FIN also doch um ein personenbezogenes Datum i.S.d. Art. 4 Nr. 1 DSGVO handeln.[31] Dies wäre dann der Fall, wenn derjenige, der Zugang zur FIN hat, zusätzlich über Mittel verfügt, die es ihm ermöglichen, die FIN zur Identifizierung des Halters, auf den

29 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 46.

30 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 47.

31 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 48.

sich die FIN bezieht, zu nutzen.[32]
Somit unterstreicht das Gericht mit seiner Entscheidung zunächst einmal deutlicher die Lehre vom relativen Personenbezug. Ob im vorliegenden Fall eine Identifizierung für den Gesamtverband möglich ist, prüft der EuGH jedoch nicht selbst, sondern überlässt diese Untersuchung dem vorlegenden Gericht.[33]
Bemerkenswert ist jedoch außerdem ein entscheidender Nebensatz des EuGHs: Wenn die FIN für einen der unabhängigen Wirtschaftsakteure, die Zugang zu dieser begehren, bei vernünftiger Betrachtung der Mittel ein personenbezogenes Datum darstellt, dann solle dies auch mittelbar für die Fahrzeughersteller, die die FIN bereitstellen, gelten.[34] Mit dem relativen Ansatz, personenbezogene Daten nur für den anzunehmen, der tatsächlich bzw. rechtlich in der Lage ist, die Person zu identifizieren, ist diese Auffassung unvereinbar und wirkt wie ein systemfremder Spagat zwischen relativem und absolutem Personenbezug. Gleichwohl bezieht der EuGH diese Position und begründet seine Abweichung auch nicht näher.

Eine mögliche Erklärung ergibt sich unter Zuhilfenahme der Pressemitteilung zu dem Urteil.[35] Dort heißt es: *„Diese Nummer ist als solche nicht personenbezogen. Sie wird jedoch zu einem personenbezogenen Datum, wenn derjenige, der Zugang zu ihr hat, über Mittel verfügt, die ihm die Identifizierung des Halters des Fahrzeugs ermöglichen, sofern der Halter eine natürliche Person ist.“*

Auch in der englischen Sprachfassung des Urteils heißt es statt „mittelbar“ nur noch „…constitutes personal data for them, within the meaning of Article 4(1) of the GDPR, and, **indirectly,** for the vehicle manufacturers (…)“[36] Dies deutet darauf hin, dass der EuGH sich in der deutschen Fassung lediglich einer unglücklichen Formulierung bedient und die hiermit verbundenen Rechtsfolgen nicht beabsichtigt. Vielmehr stellt diese Formulierung dann eine Wiederholung des bereits Bekannten dar: Sowohl für Hersteller als auch für Empfänger der FIN kommt es auf etwaige zusätzliche Mittel an, um einen Personenbezug anzunehmen. Eine Wechselwirkung zwischen beiden wäre dann aber nicht beabsichtigt.
Unter der Prämisse, dass das LG Köln einen Personenbezug annimmt, wäre die Verpflichtung zur Herausgabe der Daten an die unabhängigen Wirtschaftsakteure nach Art. 61 Abs. 1 der Verordnung 2018/858 sodann eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 lit. c DSGVO und diese wären als Empfänger auch Verantwortliche i.S.v. Art. 4 Nr. 7 DSGVO.[37]

Insgesamt hat der EuGH also seine nach der Entscheidung in der Rechtssache Breyer ausufernde Auslegung der „vernünftigerweise einsetzbaren Mittel“ weiter eingefangen und damit praxistauglicher gemacht. Es kommt also nun auf die Mittel an, die dem Verantwortlichen auch wirklich zur Verfügung stehen.[38]

Einen echten Erkenntnisgewinn bietet das Urteil darüber hinaus jedoch nicht. Der nun erstmals auftauchende „mittelbare Personenbezug“ für den Bereitsteller der Daten ist systemfremd und wäre für eine rechtssichere Prüfung des Personenbezugs kaum handhabbar.

Auch ob die FIN nun tatsächlich personenbezogene Daten darstellt oder nicht, bleibt weiterhin offen, sodass das Urteil des LG Köln mit Spannung abzuwarten ist. Allerdings lässt sich die bloße FIN kaum sinnvoll isoliert verarbeiten, sodass es naheliegt, dass etwaiges Zusatzwissen zur Identifizierung vorliegt.

Nach der erneuten Absage an die Aufsichtsbehörden bezüglich des absoluten Personenbezugs wird der Konflikt somit nur auf eine neue, tiefere Ebene verlagert. Jetzt werden die Aufsichtsbehörden die vernünftigerweise einsetzbaren Mittel entsprechend weit auslegen, mit demselben Ergebnis: Einem sehr weitgehenden Anwendungsbereich der DSGVO zum Preis einer gewissen Rechtsunsicherheit für die Praxis.

---

32 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 49.

33 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 49.

34 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 49.

35 PRESSEMITTEILUNG Nr. 168/23.

36 Hervorhebung durch den Autor.

37 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 62.

38 EuGH Urteil vom 09. November 2023, C 319/22 Rz. 46.

Vor diesem Hintergrund bleibt die mangelnde Festlegung des EuGHs in dieser Rechtssache hinter den Erwartungen an das Urteil zurück.

V. Erkenntnisse zum Personenbezug von Daten, Fazit für die Forschung

Zwischen dem absoluten und dem relativen Verständnis zum Personenbezug hat die Rechtsprechung also sukzessive eine Kompromisslösung entwickelt: Entscheidend ist, ob der jeweilige Akteur mit vernünftigen Mitteln einen Personenbezug herstellen kann. Diese Mittel können entweder rechtliche oder tatsächliche, jedoch keine illegalen Mittel sein. Wie weit die Auslegung dieser Mittel letztlich reicht, wird auch in Zukunft Gegenstand der Rechtsprechung sein, die eine auch für die Praxis handhabbare Kasuistik erarbeiten wird.

Hochschulen und Forschungseinrichtungen verarbeiten selbst in vielfältigster Gestaltung Daten. Eine genaue Bestimmung, ob diese personenbezogen sind oder nicht, ist daher von immenser Bedeutung, um die Compliance Anforderungen der DSGVO zu erfüllen und Haftungsfälle sowie Reputationsschäden zu vermeiden. Als Verantwortliche sind sie etwa selbst Adressaten der Ansprüche auf Auskunft ihrer Beschäftigten (als Arbeitgeber), Studenten (als Bildungseinrichtung) oder z. B. Studienteilnehmer (als Forschungseinrichtung). Gleichzeitig sind sie aber auch Adressat der Free-Flow-of-Data Verordnung und dürfen nichtpersonenbezogene Daten somit auch im grenzüberschreitenden Datentransfer überall im europäischen Binnenmarkt verarbeiten. Schon allein hierfür ist eine saubere Abgrenzung im Einzelfall erforderlich.

DFN Infobrief-Recht-Aktuell

AI-Act der Europäischen Union:

Die wahrscheinlich längste Trilog-Verhandlung in der Geschichte der EU hat ihren Abschluss gefunden. Damit steht das weltweit erste Gesetz zur Regulierung von Künstlicher Intelligenz weitgehend fest. Die noch ausstehende Zustimmung durch Parlament und Rat gilt als Formalität. Anwendungen, die mit künstlicher Intelligenz arbeiten, sind ab Inkrafttreten der Verordnung zu klassifizieren und die damit steigenden Regulierungsanforderungen einzuhalten. In den Verhandlungen wurde unter anderem die Definition des KI-Systems an die der OECD angepasst. Auch Basismodelle (wie z.B. ChatGPT) sind von der Regulierung betroffen.

Pressemitteilung des Rats der EU abrufbar unter:
https://www.consilium.europa.eu/de/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/ (zuletzt abgerufen am 21.12.2023).

Zum Verordnungsentwurf und zum Standpunkt des Rats der EU erschien im Januar 2023 ein Infobrief von Justin Rennert unter dem Titel „One KIss is all it takes“.
Abrufbar unter: https://www2.dfn.de/fileadmin/3Beratung/Recht/1infobriefearchiv/2023/Infobrief_Recht_01-2023.pdf

EuGH zum Schufa-Scoring

Der EuGH hat sich in einem Vorabentscheidungsverfahren zur Zulässigkeit des Scorings durch die SCHUFA geäußert (Urteil vom 07. Dezember 2023, Az.: C-634/21). Vom Verwaltungsgericht Wiesbaden wurde ihm die Frage vorgelegt, ob dem Scoring durch die SCHUFA Art. 22 Abs. 1 DSGVO entgegensteht. Der EuGH antwortete daraufhin, dass dies der Fall ist, wenn es vom automatisiert erstellten Wahrscheinlichkeitswert „maßgeblich“ abhängt, ob ein Dritter mit der Person einen Vertrag schließt oder nicht. Damit ist das Verfahren aber noch nicht abgeschlossen. Es liegt nun am Verwaltungsgericht Wiesbaden zu beurteilen, ob der durch die SCHUFA ermittelte Score-Wert „maßgeblich“ für den Vertragsabschluss ist.

Zur Vorlage durch das Verwaltungsgericht Wiesbaden und zur Rechtslage hinsichtlich des Scorings erschien im Juni 2023 ein Infobrief von Ole-Christian Tech unter dem Titel „Scoring – bald nur noch als Entscheidung auf dem Platz?“

Abrufbar unter: https://www2.dfn.de/fileadmin/3Beratung/Recht/1infobriefearchiv/2023/Infobrief_Recht_06-2023.pdf

Kurzbeitrag: Risiken und Nebenwirkungen? Jugendgefährdend und gesundheitsschädlich!

US-Bundesstaaten klagen den Meta-Konzern an

von Johanna Voget

Im Oktober 2023 haben 41 US-Bundesstaaten Klage gegen Meta erhoben. Dem Konzern wird vorgeworfen, seine sozialen Netzwerke und Online-Dienste so zu gestalten, dass Kinder und Jugendliche abhängig werden und ihrem Selbstwertgefühl Schaden zugefügt wird. Die seelische Gesundheit von minderjährigen Nutzer:innen und die Taktiken des Meta-Konzerns sind bereits seit einigen Jahren immer wieder Gegenstand der Berichterstattung und zahlreicher Verfahren.

I. Hintergrund der Klage

Die öffentliche Aufmerksamkeit für die Auswirkungen sozialer Medien auf die psychische Gesundheit von Kindern erreichte bereits 2021 einen Höhepunkt, als Frances Haugen, eine ehemalige Mitarbeiterin Metas, die zur Whistleblowerin wurde, interne Dokumente veröffentlichte. Aus diesen ging hervor, dass Instagram das Körpergefühl und Schönheitsideal von Jugendlichen, insbesondere junger Frauen, verschlechterte und dass sich der Konzern dessen bewusst war.[1] Diese Enthüllungen führten zu einer Anhörung im Kongress über die Auswirkungen der sozialen Medien auf junge Menschen

Auch Präsident Joe Biden ging in seiner Rede zur Lage der Nation im Februar 2023 auf die negativen Auswirkungen der sozialen Medien auf die psychische Gesundheit junger Nutzer:innen ein und forderte den Kongress auf, eine parteiübergreifende Gesetzgebung zur Lösung des Problems zu verabschieden.

Anfang dieses Jahres reichten Anwälte, die mehr als 100 US-amerikanische Familien vertreten, eine Sammelklage ein, in der sie Meta, Snapchat, Google und die Muttergesellschaft von TikTok, ByteDance, beschuldigten, jungen Menschen mit ihren Produkten zu schaden. Das Verfahren ist noch nicht abgeschlossen.

Nun wird die Geschichte um ein neues Kapitel ergänzt: Im Oktober 2023 wurde eine Klage von zunächst 33 US-Bundesstaaten vor dem Bundesgericht in Oakland, Kalifornien, eingereicht.[2] Weitere Bundesstaaten haben sich dieser angeschlossen.[3] In der Klageschrift wird vorgetragen, dass Meta die Öffentlichkeit wiederholt über die erheblichen Gefahren seiner Plattformen getäuscht und junge Kinder und Jugendliche wissentlich zu einer süchtig machenden und zwanghaften Nutzung sozialer Medien verleitet habe. Das zentrale Motiv des Konzerns sei der Profit. Mit der Klage wird eine Reihe von Abhilfemaßnahmen gefordert, darunter auch erhebliche Zivilstrafen.

Meta erklärte in einer Stellungnahme, dass es sich für die Sicherheit von Jugendlichen im Internet einsetze: „Wir sind enttäuscht,

1 MMR-Aktuell 2021, 442768.

2 https://www.washingtonpost.com/documents/b68f2951-2a4b-4822-b0fb-04238703c039.pdf?itid=lk_inline_manual_5 (zuletzt abgerufen am 11.12.2023).

3 https://www.zeit.de/digital/2023-10/facebook-meta-us-bundesstaaten-klage-kinder-jugendliche-psychische-gesundheit (zuletzt abgerufen am 11.12.2023).

dass die Generalstaatsanwälte diesen Weg gewählt haben, anstatt produktiv mit Unternehmen aus der gesamten Branche zusammenzuarbeiten, um klare, altersgerechte Standards für die vielen Apps zu schaffen, die Jugendliche nutzen.“ [4]

II. Ausblick und weitere Regulierung in der EU

In der EU wurden durch die Verabschiedung des Digital Services Act (DSA) bereits Regulierungen im Bereich der Verantwortlichkeit von sozialen Netzwerken als Intermediären vorgenommen.[5] Der DSA nimmt zwar nicht explizit den Jugendschutz in den Fokus, jedoch werden die Betreiber von sozialen Netzwerken in die Verantwortung genommen, konsequent gegen illegale Inhalte vorzugehen, über Risiken für Nutzer:innen zu informieren und entsprechende Maßnahmen zu ergreifen. Erste Regulierungsansätze in Deutschland sah bereits das Netzwerkdurchsetzungsgesetz aus 2017 vor, das nunmehr ab 2024 durch den DSA ersetzt wird. Dennoch ist das Thema Jugendschutz und die Auswirkung von Medien und sozialen Netzwerken auch in der EU und in Deutschland immer wieder Gegenstand von Diskussionen. Es ist nicht zu erwarten, dass die Regulierungen durch den DSA den Risiken vorbeugen und einen effektiven Schutz gewährleisten können. Im Ergebnis dürften daher künftig weitere Regelungen auf dem Gebiet erforderlich sein.

4 https://www.theguardian.com/technology/2023/oct/24/instagram-lawsuit-meta-sued-teen-mental-health-us (zuletzt abgerufen am 11.12.2023).

5 Zu den konkreten Regelungen des DSA vgl. Rennert, Brüssel reguliert das schon, DFN Infobrief Recht 06/2022.

Impressum

Der DFN-Infobrief Recht informiert über aktuelle Entwicklungen in Gesetzgebung und Rechtsprechung und daraus resultierende mögliche Auswirkungen auf die Betriebspraxis im Deutschen Forschungsnetz.

Herausgeber

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

Redaktion

Forschungsstelle Recht im DFN
Ein Projekt des DFN-Vereins an der WESTFÄLISCHEN WILHELMS-UNIVERSITÄT, Institut für Informations-, Telekommunikations- und Medienrecht (ITM), Zivilrechtliche Abteilung
Unter Leitung von Prof. Dr. Thomas Hoeren
Leonardo-Campus 9
D-48149 Münster
E-Mail: recht@dfn.de

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