„Weggeforscht“ der Podcast der Forschungsstelle Recht

Alle Informationen am Ende der Ausgabe

infobrief recht

10 / 2023
Oktober 2023

Brave New (Data) World?

Datenschutzrecht im Metaverse

Kommt es nicht auf die inneren Werte an?

Kritik an der momentanen Praxis des E-Lendings – ein Überblick zum Reformbedarf des Urheberrechts bzgl. der Ausleihe von E-Books

Das neue Data Privacy Shamework?

Der neue Angemessenheitsbeschluss für Datenexporte in die USA liegt vor

Kurzbeitrag: Was kratzt mich das?

OLG Hamm: Scraping-Vorfälle bei Facebook rechtfertigen keinen DSGVO-Schadensersatz

Brave New (Data) World?

Datenschutzrecht im Metaverse

von Johanna Voget

Das Metaverse – ein Buzzword, das ebenso wie die Künstliche Intelligenz (KI) derzeit in aller Munde ist. Viele Fragen sind noch offen: Was ist das Metaverse überhaupt und wie wird es sich auf die Gesellschaft, Wirtschaft und das alltägliche Leben auswirken? Auch die rechtlichen Implikationen der neuen Technologie rund um die entstehenden virtuellen Realitäten werden bereits viel diskutiert. Dieser Beitrag soll sich nun einem Teil der Problemfelder widmen und das Datenschutzrecht im virtuellen Raum näher beleuchten.

I. Begriff und Komponenten des Metaversums

„Das Metaverse“ gibt es so tatsächlich noch gar nicht. Die Bezeichnung soll einen Zusammenschluss verschiedener virtueller Realitäten erfassen, zwischen denen die Nutzenden wechseln können.[1] Die virtuellen Realitäten selbst und die Technologie dahinter stellen grundsätzlich schlicht eine Weiterentwicklung des Internets dar, das sog. Web 3.0. Während die Nutzenden das derzeit existente Web 2.0 schon teilweise selbst mitgestalten können, also beispielsweise in sozialen Netzwerken wie TikTok, Instagram oder Twitter eigene Inhalte kreieren und darstellen können, soll dies im Web 3.0 noch verstärkt werden unter gleichzeitiger Dezentralisierung der Plattformen und Schaffung von Interoperabilität zwischen selbigen. Möglich wird dies durch die Entwicklung der sog. Distributed Ledger Technologie, die der Blockchain zugrunde liegt. Neu ist auch, dass die Nutzenden in die virtuelle Umgebung in ihrer dreidimensionalen Ausgestaltung „eintauchen“ und sich dort verkörpert durch Avatare fortbewegen können. Relevanz entfaltet das Metaverse aber nicht nur für den Privatgebrauch – grade im Bereich von Wirtschaft und Kultur verzeichnet die virtuelle Welt derzeit die größten Entwicklungen. So haben sich bereits zahlreiche Unternehmen ihre virtuelle Präsenz auf Plattformen wie Decentraland erschaffen, in denen sie sich und ihre Produkte darstellen und bewerben können. Virtuelle Grundstücke und Immobilien werden zu hohen Preisen verkauft und sind sehr begehrt. Darüber hinaus fanden bereits vielfältige Modeschauen, Konzerte und Kunstausstellungen im virtuellen Raum statt. Auch im Bereich der Bildung soll die virtuelle Realität Nutzen stiften. Angestoßen durch die pandemiebedingte Verlagerung des Lernens in den digitalen Raum, sollen Schüler und Studierende durch die Dreidimensionalität und Ortsungebundenheit der virtuellen Umgebung profitieren. [2]

II. Datenschutzrechtliche Fragestellungen

Grundsätzlich hat jeder durch die Registrierung bei einer der Plattformen die Möglichkeit, die virtuellen Realitäten zu nutzen. Die Nutzung und Ausgestaltung des Metaverse führt (wenig überraschend) zu einem weiteren Datenverarbeitungsfeld, das gegenüber dem digitalen Bereich wohl noch deutlich gesteigerte Ausmaße annimmt. Dabei ist das Metaverse kein rechtsfreier Raum, in dem keine datenschutzrechtlichen Anforderungen zu erfüllen sind. Im Folgenden wird daher die Anwendbarkeit der Datenschutzgrundverordnung (DSGVO) im virtuellen Raum, sowie die daraus resultierenden möglichen Verantwortlichkeiten und Pflichten einer eingehenden Prüfung unterzogen, um darzustellen, was Datenschutz im Metaverse bedeutet und welche Probleme sich hierbei ergeben.

1 https://www.handelsblatt.com/technik/metaverse-was-hinter-dem-metaverse-hype-steckt/28073180.html (zuletzt abgerufen 19.09.23).

2 https://scholar.harvard.edu/mcgivney/new-report-introduction-learning-metaverse (zuletzt abgerufen 19.09.23).

1. Anwendbarkeit der DSGVO

Die Frage, welches Recht Anwendung findet, ist im Kontext virtueller Realitäten generell von hoher Relevanz. So ist auch für die Zwecke dieses Beitrags, zunächst zu fragen, ob und in welchem Umfang die DSGVO auf die datenschutzrechtlichen Fragen im virtuellen Raum überhaupt anzuwenden ist. Ebenso wie bereits im Zusammenhang mit jeder Fallgestaltung in der jetzigen Form des Internets, ist eine geografische Anknüpfung der Tätigkeiten von Akteuren nur erschwert möglich. Im Metaverse gibt es keine Grenzen. Vielmehr treffen hier Unternehmen und Einzelpersonen aus allen Ländern der Welt aufeinander, sodass eine aufmerksame kollisionsrechtliche Prüfung erforderlich ist.

a) Sachliche Anwendbarkeit

Gem. Art. 2 Abs. 1 DSGVO ist für die Anwendbarkeit der DSGVO Voraussetzung, dass eine Verarbeitung von personenbezogenen Daten vorliegt. Als personenbezogene Daten sind nach Art. 4 Nr. 1 DSGVO alle Informationen zu verstehen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Hier wird für die virtuelle Realität verwendete Hardware relevant. Sog. Virtual-Reality (VR) Brillen verarbeiten zunächst Daten über die reale Umgebung des Nutzenden, wodurch auch Dritte und sich auf diese beziehende Daten betroffen sein können.
Darüber hinaus sind sowohl einige VR-Brillen als auch andere Hardwarekomponenten, wie spezielle Haptikanzüge, in der Lage, Daten wie Mimik, Gestik oder andere körperliche Reaktionen zu erkennen und auszuwerten. Werden solche Daten zur Identifizierung einer Person genutzt, handelt es sich sogar um eine besondere Kategorie personenbezogener Daten nach Art. 9 Abs. 1 DSGVO.
Außerdem werden auch durch die Aktivität des Nutzenden in der virtuellen Welt Daten generiert, die Personenbezug aufweisen können. Eine Identifizierung des Nutzenden kommt so über den Namen des Avatars, über dessen ID oder dessen Handlungen in Betracht.[3]

Vom Anwendungsbereich ausgenommen ist die Datenverarbeitung gem. Art. 2 Abs. 2 DSGVO für rein private oder familiäre Tätigkeiten.
Unproblematisch lässt sich hingegen die Verarbeitung personenbezogener Daten im Rahmen von geschäftlichen Handlungen im Metaverse bejahen, wie beispielsweise bei der Nutzung von Kreditkartendaten, E-Mail-Adressen, Wallet-Adressen, Lieferadressen oder anderen vom Nutzenden bereitgestellte Daten.

b) Räumliche Anwendbarkeit

Darüber hinaus findet die DSGVO in räumlicher Hinsicht nach dem Niederlassungs- und Marktortprinzip gem. Art. 3 Abs. 1 und 2 DSGVO Anwendung. Danach ist zum einen die Verarbeitung personenbezogener Daten erfasst, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung selbst in der Union stattfindet (Art. 3 Abs. 1 DSGVO). Zum anderen ist die Verarbeitung personenbezogener Daten von betroffenen Personen umfasst, die sich in der Union befinden, auch wenn der Verantwortliche oder Auftragsverarbeiter nicht in der Union niedergelassenen ist, wenn die Datenverarbeitung im Zusammenhang mit dem Angebot von Waren und Dienstleistungen an die betroffenen Personen oder der Beobachtung des Verhaltens der betroffenen Personen steht (Art. 3 Abs. 2 DSGVO).

Hat der Anbieter der virtuellen Plattform also seinen Sitz im Unionsgebiet ist eine Anwendung der DSGVO nach dem Niederlassungsprinzip unproblematisch gegeben. Ist er in einem Drittstaat ansässig (wie beispielsweise in den USA, wo derzeit die meisten Gründer von Metaverse-Plattformen agieren), ist zu prüfen, ob sich ihre Tätigkeit auf den europäischen Markt und die hier ansässigen Nutzenden auswirkt. Dazu ist unter anderem die inhaltliche Ausgestaltung des Angebots zu bewerten, wie die Sprache, Währung oder mögliche Versandangebote.[4]

2. Verantwortlichkeit

Findet die DSGVO auf die betreffende Fallgestaltung in der virtuellen Realität Anwendung, ist in einem zweiten Schritt zu prüfen, wen die datenschutzrechtlichen Pflichten treffen, wer also als Verantwortlicher i.S.d. DSGVO anzusehen ist. Da das Web 3.0 von einer Vielzahl von Akteuren mitgestaltet wird bzw. werden soll, stellt sich die Beurteilung der datenschutzrechtlichen Verantwortlichkeit als komplex dar.

3 Kaulartz/Schmid/Müller-Eising, RDi 2022, 521 (526).

4 Bender-Paukens/Werry, ZD 2023, 127 (129).

Zunächst ist dabei die Struktur der Plattform entscheidend. Ist die Plattform zentral organisiert, wie beispielsweise Horizon von Meta oder Fortnite von Epic Games, und werden durch diese zentralen Betreiber auch die Zwecke und Mittel der Datenverarbeitung i.S.v. Art. 4 Nr. 7 DSGVO festgelegt, handeln diese als Verantwortliche.[5]

Mit Blick auf die Fanpage-Entscheidung des EuGH[6] kommen jedoch auch gemeinsame oder getrennte Verantwortlichkeiten in Betracht. So stellt sich bei bei virtuellen Geschäftsräumen oder Einrichtungen beispielsweise die Frage, ob der Inhaber des Grundstücks, gleichsam der Hausrechtsinhaber, auch als Verantwortlicher anzusehen ist, wenn ein Nutzender in Gestalt seines Avatars das Grundstück betritt und eine Interaktion dergestalt stattfindet, dass personenbezogene Daten durch den Grundstücksinhaber verarbeitet werden.

Hier dürfte eine Prüfung im Einzelfall erforderlich sein, wer über das Mittel („wie") und Zwecke („warum") einer Verarbeitung von personenbezogenen Daten bestimmt (gem. Art. 26 Abs. 1 S. 1 DSGVO). Die tatsächliche Einflussnahme der Datenverarbeiter im Metaverse ergibt sich in diesen Fällen mithin im Einzelfall durch eine funktionelle Betrachtungsweise.

Ist der virtuelle Raum dezentral aufgebaut, wie langfristig für das gesamte Metaverse geplant, stellt sich die Frage der datenschutzrechtlichen Verantwortlichkeit für die jeweiligen Betreiber der Server und Nutzer der Plattform einzeln. Es muss jeweils geprüft werden, ob ein Teilnehmer des dezentralen Netzwerkes personenbezogene Daten für eigene Zwecke und Mittel verarbeitet.[7] Hat das betreffende Unternehmen oder die Institution hingegen lediglich eine virtuelle Präsenz im Metaverse, bei der keine Interaktionsmöglichkeiten mit den Nutzenden bestehen, dürfte eine Verantwortlichkeit abzulehnen sein.

3. Datenschutzrechtliche Pflichten und Anforderungen

Die jeweiligen Verantwortlichen müssen sodann die ihnen obliegenden Pflichten und Anforderungen nach der DSGVO erfüllen. Danach trifft sie der bekannte weitreichende Pflichtenkatalog, der beispielsweise Informations-, Auskunfts- und Meldepflichten beinhaltet. Während im Web 2.0 die Datenschutzinformationen, wie die Benennung des Verantwortlichen und bestehende Betroffenenrechte, üblicherweise in einem Impressum mitgeteilt werden, müssen diese im Metaverse dem Nutzenden ebenfalls in der konkreten Interaktion in irgendeiner Form zur Verfügung gestellt werden. Möglich wäre dies in dem Szenario, wenn er in Gestalt seines Avatars ein Geschäft oder eine Einrichtung betritt. Natürlich ist auch in der virtuellen Realität jede Datenverarbeitung rechtfertigungsbedürftig. In einigen Bereichen kann die Datenverarbeitung durch ausdrückliche Einwilligung des Nutzenden gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO gerechtfertigt sein, wenn der Nutzende bei seiner Registrierung auf der Plattform diese erteilt. Soweit geschäftliche Interaktionen vorliegen, wie im Rahmen des Angebots und Erwerbs von Waren oder Dienstleistungen zwischen einem Unternehmer und einem Nutzenden, kann sich die Rechtmäßigkeit der Datenverarbeitung darüber hinaus aus Art. 6 Abs. 1 S. 1 lit. b DSGVO ergeben.[8]

Darüber hinaus haben die Betreiber bereits bei der Entwicklung einer virtuellen Plattform oder der Gestaltung von Produkten und Dienstleistungen für den virtuellen Raum die Vorgaben des Datenschutzes durch Technikgestaltung (Data Protection by Design) und durch datenschutzrechtliche Voreinstellungen (Data Protection by Default) i.S.d. Art. 25 DSGVO einzuhalten. Auch müssen sie geeignete technische und organisatorische Maßnahmen (TOM) treffen, damit die Grundsätze der DSGVO wirksam gewährleistet werden können.

Hinzu kommen Anforderungen an die Sicherheit der Daten nach Art. 32 DSGVO sowie an den Transfer von personenbezogenen Daten in Drittländer. Gerade vor dem Hintergrund der von den Metaverse-Experten versprochenen Interoperabilität der virtuellen Plattformen und Verschmelzung zu einem

5 Kaulartz/Schmid/Müller-Eising, RDi 2022, 521 (526).

6 EuGH NJW 2018, 2537.

7 Kaulartz/Schmid/Müller-Eising, RDi 2022, 521 (526).

8 Klar/Wegmann/Galandi, BB 2022, 2691 (2694).

gesamtheitlichen Metaverse, ist ein internationaler Datentransfer nahezu zwingend. Hier sind die durch die Schrems-Verfahren entwickelten Hürden und Anforderungen der Rechtsprechung zu beachten und die Entwicklung abzuwarten.[9]

III. Ein Blick über den Tellerrand (der DSGVO) hinaus

Neben der DSGVO gilt es möglicherweise noch weitere Rechtsakte der EU im Bereich des Datenschutzes in den Blick zu nehmen, über die die Forschungsstelle Recht bereits in der Vergangenheit informierte.[10] So sieht der Digital Services Act (DSA) einheitliche Regelungen hinsichtlich der Haftung und Sicherheitsvorkehrungen für Online-Plattformen vor, welche sich auch auf Metaverse-Plattformen anwenden lassen. Sobald sich auch im Web 3.0 führende Akteure herausbilden sollten, gilt es auch den Digital Marktes Act (DMA) zu beachten, der sich an sog. Gatekeeper richtet.

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Während sich die Technologie und Ausgestaltung virtueller Realitäten derzeit noch in der Entwicklung befindet und die Plattformen derzeit überwiegend von Akteuren der Wirtschaft in Anspruch genommen und getestet werden, ist auch eine Präsenz von Hochschulen und Forschungseinrichtungen im Metaverse in nicht allzu ferner Zukunft. In der virtuellen Umgebung ergeben sich zahlreiche neue Möglichkeiten und Chancen für Bildung und Forschung. Bei einer Nutzung der virtuellen Räume ist sodann die Einhaltung der datenschutzrechtlichen Bestimmungen unerlässlich. Agiert eine in der EU ansässige Hochschule oder Forschungseinrichtung im Metaverse kann die DSGVO auf die Verarbeitung von personenbezogenen Daten in diesem Kontext Anwendung finden und die Einrichtung selbst als Verantwortliche betreffen, sodass die Ausgestaltung und Umsetzung des eigenen virtuellen Angebots immer mit Blick auf das Datenschutzrecht erfolgen muss.

---

9 EuGH NJW 2015, 3151; EuGH NJW 2020, 2613; Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 08/2020; Nickoleit, Der Tragödie letzter Teil?, DFN-Infobrief 05/2021; McGrath, Ausgeschremst?, DFN-Infobrief Recht 05/2022.

10 Rennert, Brüssel reguliert das schon, DFN-Infobrief Recht 06/2022.

Kommt es nicht auf die inneren Werte an?

Kritik an der momentanen Praxis des E-Lendings – ein Überblick zum Reformbedarf des Urheberrechts bzgl. der Ausleihe von E-Books

von Johannes Müller

Die bestehenden Regelungen zur Ausleihe von E-Books unterscheiden sich substantiell von der Rechtslage zur Ausleihe von körperlichen Büchern. Insbesondere Bibliotheken sehen die derzeitige Praxis des E-Lendings als unbefriedigend an. Eine mögliche Reform des E-Lendings ist Teil des politischen Diskurses.

I. Der Ursprung der Kritik am E-Lending

Die Kritik an der derzeitigen Praxis des E-Lendings findet ihren Ursprung in den Abweichungen zum Verleih von körperlichen Büchern. Diese unterschiedliche Praxis lässt sich auf die verschiedenen urheerrechtlichen Rahmenbedingungen für die beiden Verleihformen zurückführen.[1] Um sie zu verstehen, gilt es daher zunächst die Rechtslage rund um die Verleihung von körperlichen Büchern aufzuzeigen und hiernach die juristischen Herausforderungen des E-Lendings darzustellen.

II. Die Erschöpfung des Verleihrechts des Urhebers bei körperlichen Büchern

Die Grenzen der Nutzung von fremden urheberrechtlich geschützten Werken, wie Büchern, finden sich in den §§ 12 ff. Urheberrechtsgesetz (UrhG). Hierbei regeln die §§ 14 ff. UrhG, das grundsätzlich nur der Urheber das Recht hat, die von ihm geschaffenen Werke zu verwerten. Zu den Verwertungsrechten der Urheber zählt auch das Verbreitungsrecht gemäß § 17 UrhG. Nach § 17 UrhG ist grds. nur der Urheber berechtigt, sein Werk oder Kopien von diesem in den Verkehr zu bringen. Das alleinige Verbreitungsrecht des Urhebers wird jedoch durch den Erschöpfungsgrundsatz in § 17 Abs. 2 UrhG begrenzt. Sofern ein urheberrechtlich geschütztes Werk mit der Zustimmung des Urhebers in den Verkehr gelangt ist, darf dieses spezifische Werkstück auch weiterverbreitet werden, ohne dass hierbei das Urheberrecht verletzt wird. Dies bedeutet in der Praxis, dass etwa der Autor eines Buches nur das Recht hat, über den Erstverkauf des Buches zu bestimmen und hiervor finanziell zu profitieren. Sofern ein Exemplar dieses Buches verkauft wurde, kann der Erwerber dieses Exemplar weiterverkaufen ohne hierbei die Urheberrechte des Autors zu verletzen. Der Erschöpfungsgrundsatz bezieht sich gemäß § 17 Abs. 2 UrhG jedoch nicht auf die Vermietung des in den Verkehr gebrachten Werks. Der Käufer eines Buches hat also nicht das Recht dieses (gegen Entgelt) an andere weiterzuvermieten, sofern ihm nicht zuvor vom Urheber das Recht zur Vermietung separat eingeräumt wurde. Vom Vermietrecht zu unterscheiden ist allerdings das Leihrecht. Anders als Vermietrecht erschöpft sich das Verleihrecht des Urhebers an körperlichen Werken gemeinsam mit dem Verbreitungsrecht, wenn das Werk in den Verkehr gebracht wurde. Der Käufer eines Buches darf dasselbe Buch also nicht vermieten, allerdings verleihen, ohne dass er sich hierfür Nutzungsrechte vom Urheber einräumen lassen muss. Zur Differenzierung zwischen Vermietung und Verleihung ist gemäß § 17 Abs. 3 UrhG zu fragen, ob die Gebrauchsüberlassung Erwerbszwecken dient. Ist dies der Fall, erfolgt die Gebrauchsüberlassung also aus wirtschaftlichem Interesse, ist eine Vermietung gegeben. Andersherum liegt eine Verleihung vor, sofern der Verleiher hiermit keine wirtschaftlichen Interessen verfolgt. Sofern lediglich ein Entgelt erhoben wird, das der Kostendeckung dient und keine Gewinne erzielen soll, liegt ebenso eine Verleihung vor. Daher können sich Bibliotheken auf die Erschöpfung des Verleihrechts berufen, die Bücher – ohne oder zu nur geringem Entgelt zur Kostendeckung – verleihen. Sie verletzen nicht das Verwertungsrecht des Urhebers und müssen

1 Vgl. hierzu Gielen, Bis hierher und nicht weiter, DFN-Infobrief Recht 05/2020.

keine Nutzungsrechte erwerben. Allerdings sind Bibliotheken dazu verpflichtet, die Urheber für den Verlust der potentiellen Vergütungsmöglichkeiten zu entschädigen. Hierzu regelt § 27 Abs. 2 UrhG, dass bei der Verleihung eines Werkes durch eine öffentlich zugängliche Einrichtung der Urheber einen Anspruch auf eine angemessene Vergütung hat.
Es kann also für körperliche Bücher zusammengefasst werden, dass Bibliotheken, die ein Buch erwerben, auch das Recht haben, dieses zu verleihen. Hierfür müssen sie keine zusätzlichen Rechte vom Urheber einholen, der Urheber kann das Verleihen des Buches somit auch nicht verbieten. Allerdings sind Bibliotheken als öffentlich zugängliche Einrichtungen dazu verpflichten den Urheber angemessen zu entschädigen, wenn sie seine Bücher verleihen.

III. Der Verleih von E-Books als öffentliche Zugänglichmachung

Der Erschöpfungsgrundsatz gemäß § 17 Abs. 2 UrhG bezieht sich bei Büchern jedoch nur auf körperliche Werke. Die unkörperliche Verwertung von E-Books ist hiervon nicht erfasst. Bibliotheken, die E-Books verleihen möchten, können sich nicht darauf berufen, dass das Verleihrecht des Urhebers an einem E-Book durch den Verkauf erloschen ist. Der Verleih von E-Books wird nach deutschem Recht als Form der unkörperlichen öffentlichen Wiedergabe gemäß § 15 Abs. 2 UrhG angesehen, spezifischer als Fall der öffentlichen Zugänglichmachung gemäß § 19a UrhG. Hiernach steht alleine dem Urheber das Recht zu, sein Werk der Öffentlichkeit zugänglich zu machen. Möchten Bibliotheken E-Books verleihen, müssen sie hierfür ein Nutzungsrecht vom Ur-heber gegen Entgelt erwerben. Der zentrale Unterschied zum Verleih von körperlichen Büchern liegt also darin, dass Bibliotheken darauf angewiesen sind, dass die Autoren ihnen das Recht zur Verleihung von E-Books einräumen. Ob diese Rechteeinräumung erfolgt, liegt im alleinigen Ermessen der Urheber, die im Gegensatz zu körperlichen Büchern folglich auch die Möglichkeit haben, den Verleih von E-Books vollkommen zu unterbinden.

IV. Die derzeitige Praxis des E-Lendings

Nach der heutigen Rechtslage sind also Bibliotheken dazu verpflichtet Nutzungsrechte von den Autoren bzw. den Verlagen, denen regelmäßig umfangreiche Verwertungsrechte von den Autoren eingeräumt wurden, für E-Books zu erwerben. Der Erwerb der Lizenzen erfolgt teilweise über Aggregatoren wie die Divibib GmbH, die mit den Verlagen Lizenzpakete für die Bibliotheken verhandeln und hierfür eine Provision (bspw. 30 Prozent) erhalten. Die Nutzungsrechte werden häufig zeitlich befristet eingeräumt oder auf eine begrenzte Anzahl von Ausleihvorgängen beschränkt. Hierdurch sollen gleichartige Ergebnisse wie beim Verleih von körperlichen Büchern erzielt werden, die aufgrund von Abnutzungserscheinungen auch nicht unendlich häufig ausgeliehen werden können. Ebenso kann regelmäßig nur ein Nutzer auf ein E-Book zugreifen. Die Verhinderung der gleichzeitigen Ausleihe eines einzelnen E-Books durch mehrere Nutzer dient ebenso dazu, vergleichbare Verhältnisse wie bei der klassischen Ausleihe von körperlichen Büchern herzustellen. Eine Vielzahl von Verlagen setzt zudem das sogenannte Windowing ein. Dies bezeichnet eine Sperrfrist zwischen dem Neuerscheinen eines Buchtitels und dem Einräumen einer Verleihlizenz. Durch diese Sperrfrist, die bis zu 12 Monate dauern kann, möchten die Verlage den Verkauf von E-Books und gedruckten Büchern fördern, indem interessierte Leser nicht die Möglichkeit erhalten, die Titel kurz nach Erscheinung als E-Book auszuleihen. Andere Buchtitel werden zudem überhaupt nicht zur Verleihung angeboten. Auch hierfür sind die Gründe wirtschaftlicher Natur oder haben ihre Ursache darin, dass bereits den Verlagen nur beschränkte Nutzungsrechte von den Autoren eingeräumt wurden. Hierauf zielt maßgeblich die Kritik von Bibliotheksverbänden ab, die in der zeitlich nachgelagerten oder fehlenden Leihmöglichkeit von neuen E-Books eine erhebliche Beschränkung der grundrechtlich geschützten Informationsfreiheit (Art. 5 Abs. 1 S. 1 Var. 2 GG) sehen.

V. Reformvorschläge fürs E-Lending

Angesichts der Kritik an der derzeitigen Praxis des E-Lending verwundern Rufe nach einer Veränderung des Urheberrechts zugunsten einer Ausweitung der E-Lending-Möglichkeiten nicht. Wie bei den meisten politischen Forderungen herrscht auch hier Uneinigkeit. Neben Stimmen, die eine Ausweitung des E-Lendings bereits nach bisherigem Recht als zulässig erachten, sprechen sich insbesondere Verlage und der kommerzielle Buchmarkt

gegen eine Reform aus.[2] Sie fürchten eine „Kannibalisierung" des Buchmarktes durch öffentliche Bibliotheken und wollen an der bisherigen Praxis des E-Lendings auf Basis von Lizenzverträgen festhalten, die es Verlagen und Autoren erlaubt, die Preise und die Zeitpunkte der Lizenzierung und die Beantwortung der Frage, ob überhaupt lizenziert wird, eigenständig festzulegen. Dem steht naturgemäß insbesondere der Deutsche Bibliotheksverband gegenüber, der schon lange eine gesetzliche Ausgestaltung des E-Lendings und eine Gleichstellung von digitalen und analogen Büchern fordert.

Konkrete Gestalt gewann ein Reformvorschlag des Bundesrats in der letzten Legislaturperiode, der Verlage dazu verpflichten sollte, Bibliotheken Nutzungsrechte für erhältliche E-Books gegen angemessene Bedingungen einzuräumen. Zu den angemessenen Bedingungen sollte insbesondere zählen, dass Bibliotheken das Recht eingeräumt wird, jeweils ein Vervielfältigungsstück des Werks digital für begrenzte Zeit jeweils einer Person zugänglich zu machen. Der Vorschlag, der auch reichlich Kritik von Verlagen und Autoren auf sich zog, setzte sich nicht durch.

Jedoch enthält auch der aktuelle Koalitionsvertrag den Hinweis auf „faire Rahmenbedingungen beim E-Lending in Bibliotheken".[3] Zur Umsetzung dieses Zieles beschäftigen sich gerade zwei Bundesbehörden mit einer möglichen Reform des E-Lendings. Das Bundesministerium der Justiz prüft den Regulierungsbedarf für den Verleih von E-Books durch Bibliotheken und hat hierzu einen Fragenkatalog erstellt, der bis Ende Juni 2023 beantwortet werden konnte.[4] Gleichzeitig hat die Beauftragte der Bundesregierung für Kultur und Medien eine Studie ausgeschrieben, die Auswirkungen des E-Lendings auf den Buchmarkt untersucht. Diese Ausschreibung resultierte aus einem Runden Tisch, der von öffentlichen Bibliotheken und der Kulturstaatsministerin ein-berufen wurde. Hieran nahmen der Börsenverein des Deutschen Buchhandels, der Deutsche Bibliotheksverband, der Verein Deutscher Bibliothekarinnen und Bibliothekare, der Verband deutscher Schriftstellerinnen und Schriftsteller, das Netzwerk Autorenrechte, der Verband deutschsprachiger Übersetzerinnen und Übersetzer literarischer und wissenschaftlicher Werke, sowie das Bundeskanzleramt, das Bundesministerium der Justiz und das Bundesministerium für Wirtschaft und Klimaschutz teil.[5]

VI. Fazit und Ausblick auf die Zukunft des E-Lendings

Die derzeitigen politischen Entwicklungen zum E-Lending sind mit Aufmerksamkeit zu beobachten. Die momentane Praxis wird insbesondere von den Bibliotheken als unbefriedigend angesehen. Sie beklagten die in Teilen fehlende Möglichkeit neue erschienene Titel unmittelbar als E-Books zu verleihen. Andere Titel werden überhaupt nicht zur Leihe als E-Book zur Verfügung gestellt. Änderungen könnten durch eine Reform des Urheberrechts mit dem Ziel einer verpflichteten Lizenzierung oder einer Erschöpfung des Verleihrechts bei in den Verkehr gebrachten E-Books erzielt werden. Hierbei müssten jedoch auch die berechtigten Interessen von Autoren, Verlagen und dem Buchhandel angemessen berücksichtigt werden.

---

2 Vgl. Initiative Fair Lesen, Schreiben ist nicht umsonst, https://www.initiative-fair-lesen.de/ (zuletzt abgerufen am 04.09.2023) und Börsenverein des deutschen Buchhandels, E-Book-Leihe in Öffentlichen Bibliotheken, https://www.boersenverein.de/politik-recht/positionen/e-book-leihe/ (zuletzt abgerufen am 04.09.2023).

3 Mehr Fortschritt wagen. Bündnis für Freiheit, Gerechtigkeit und Nachhaltigkeit. Koalitionsvertrag 2021-2025 zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90 / Die Grünen und den Freien Demokra-ten (FDP), 98, abrufbar unter https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf (zuletzt abgeru-fen am 04.09.2023).

4 Bundesministerium der Justiz, Urheberrecht, https://www.bmj.de/DE/themen/wirtschaft_finanzen/rechtschutz_urheberrecht/urheberrecht/urheberrecht_node.html (zuletzt abgerufen am 04.09.2023).

5 Bundesregierung, Erster Schritt zur Lösung der Probleme beim E-Lending in öffentlichen Bibliotheken, https://www.bundesregierung.de/breg-de/bundesregierung/bundeskanzleramt/staatsministerin-fuer-kultur-und-medien/aktuelles/erster-schritt-zur-loesung-der-probleme-beim-e-lending-in-oeffentlichen-bibliotheken-2185734 (zuletzt abgerufen am 04.09.2023).

Das neue Data Privacy Shamework?

Der neue Angemessenheitsbeschluss für Datenexporte in die USA liegt vor

Von Nicolas John

Datenexporte von personenbezogenen Daten aus den Mitgliedsstaaten der Europäischen Union (EU) in die Vereinigten Staaten (USA) sind bei vielen Software-Anwendungen der Standard. Die Gründe hierfür sind z.B. die amerikanischen Software-Anbietenden, die ihre Server auch in den USA betreiben, die internationale Vernetzung der Apps, Supporttätigkeiten oder die kommerzielle Weitergabe der Daten an Drittanbietende wie z. B. in der Werbeindustrie. Doch in den letzten Jahren war der Datenexport ein Auf und Ab der Beschlüsse: Erst Safe Harbor, dann Privacy Shield und jetzt? Dem neuen Angemessenheitsbeschluss, dem EU-US Data Privacy Framework (DPF) widmet sich dieser Beitrag.

I. Hintergrund

Die Verarbeitung personenbezogener Daten unterfällt bekanntermaßen den Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Danach ist gemäß Art. 6 DSGVO für jede Datenverarbeitung eine Rechtsgrundlage erforderlich. Nur mit Vorliegen einer solchen Verarbeitungsgrundlage ist die Datenverarbeitung rechtmäßig.

Möchten die Verantwortlichen die personenbezogenen Daten allerdings außerhalb des Geltungsbereichs der DSGVO, in einen sog. Drittstaat übermitteln, erhöhen sich die rechtlichen Anforderungen. Dann müssen sie neben den allgemein gültigen Vorgaben der DSGVO weitere, spezifische Bedingungen erfüllen.[1] Hierzu gehören entweder das Vorliegen eines Angemessenheitsbeschlusses[2], das Vorhalten geeigneter Garantien[3] oder das Vorliegen bestimmter Ausnahmetatbestände[4] wie z. B. eine ausdrückliche, einzelfallbezogene Einwilligung der betroffenen Person oder der Schutz lebenswichtiger Interessen.

Diese zusätzlichen Bestimmungen für Datenexporte dienen dazu, das Schutzniveau der europäischen DSGVO bei der Verarbeitung personenbezogener Daten europäischer Bürger:innen auch außerhalb des Geltungsbereichs der DSGVO zu erhalten. Da die Voraussetzungen der Datenübermittlung bei Vorliegen eines Angemessenheitsbeschlusses der Europäischen Kommission am geringsten sind, wird ein Datenexport auf Grundlage eines solchen Beschlusses von den Verantwortlichen regelmäßig bevorzugt.

II. Historie der Angemessenheitsbeschlüsse

Doch mit Blick auf Datenexporte in die USA hatten es die Verantwortlichen in den letzten Jahren nicht leicht. Denn der nun beschlossene Angemessenheitsbeschluss ist schon der dritte seiner Art.

Noch vor Inkrafttreten der DSGVO, unter den Regelungen der damals geltenden Datenschutzrichtlinie, war der erste Angemessenheitsbeschluss das sog. Safe-Harbor-Abkommen. Dieser wurde im Jahr 2000 zwischen der Europäischen Kommission und dem US-Handelsministerium geschlossen und diente der

1 Art. 44 DSGVO.

2 Art. 45 DSGVO.

3 Art. 46 DSGVO.

4 Art. 49 DSGVO.

Erleichterung des Datenaustauschs zwischen der EU und den USA. Das Abkommen ermöglichte Unternehmen die Selbstzertifizierung über das Vorliegen eines angemessenen Datenschutzniveaus. Dabei sah es vor, dass sich die Unternehmen, welche unter die Aufsicht der Federal Trade Commision (FTC) oder des Department of Transportation fielen, zur Einhaltung der veröffentlichten Grundsätze und der dazugehörigen FAQ verpflichten konnten. Mit einer Meldung an die FTC, oder eine von dieser benannten Stelle, konnten sie sich sodann selbst zertifizieren. Die Kommission wiederum erkannte an, dass diese Unternehmen ein angemessenes Datenschutzniveau gewährleisten.

Das Safe-Harbour-Abkommen erfuhr allerdings schon früh Kritik, die sich insbesondere auf die Einhaltung der Grundsätze der Erforderlichkeit, der Verhältnismäßigkeit und der Zweckbindung bezog. Das Ende des Abkommens besiegelte die Entscheidung des EuGHs vom 6. Oktober 2015 (C-362/14), das sog. „Schrems-I-Urteil“.[5] Der EuGH erklärte im Wege des Vorabentscheidungsverfahrens den Beschluss der Kommission für unwirksam und begründete gleichzeitig eine regelmäßige Prüfpflicht für Angemessenheitsbeschlüsse. Mit der Entscheidung fiel folgend das Safe-Harbour-Abkommen als Grundlage der Datenübermittlung in die USA weg. Als Folge legte die Kommission einen Entwurf zum sog. „EU-US Privacy Shield“ vor, welches die Defizite des Safe-Harbor-Abkommens ausgleichen sollte. Wie das Safe-Harbour-Abkommen folgte auch das Privacy Shield dem Grundprinzip der Selbstzertifizierung. Änderungen sollte es vor allem hinsichtlich des Schutzes personenbezogener Daten von EU-Bürgern geben. Daneben sollte eine intensive Überwachung durch US-Behörden verhindert werden und eine Erweiterung von Rechtschutzmöglichkeiten für EU-Bürger geschaffen werden. Die Kommission verabschiedete sodann am 12. Juli 2016 den Angemessenheitsbeschluss, welcher als neue Grundlage des Datentransfers zwischen der EU und den USA diente.

Doch auch das Privacy Shield wurde mit Urteil des EuGHs vom 16. Juli 2020 (C-311/18), dem sog. „Schrems-II-Urteil“[6], für ungültig erklärt. Insbesondere die geheimdienstlichen Überwachungsprogramme der USA waren Anknüpfungspunkt des EuGHs, um den Schutzstandard der USA für unzureichend zu erklären. Aufgrund dieser Entscheidung konnte das Privacy Shield nicht mehr als Grundlage für Exporte in die USA herangezogen werden. Diese Unwirksamkeit sorgte in der Folge für Unsicherheit im Umgang mit Datentransfers in die USA.[7]

III. Das neue EU-US Data Privacy Framework

Infolge des für ungültig erklärten Privacy Shield hat die Kommission nun am 10. Juli 2023 einen neuen Angemessenheitsbeschluss angenommen, das „EU-US Data Privacy Framework“ (DPF)[8], das nun als Grundlage für Datenübermittlung an zertifizierte Organisationen in die USA dient. Dieses soll nun endgültig die vom EuGH im Hinblick auf das Privacy Shield attestierten Probleme lösen und den USA ein weiteres Mal ein angemessenes Datenschutzniveau nach Art. 45 Abs. 3 DS-GVO durch die Kommission bescheinigen.

Doch auch dieser Beschluss hat noch vor Inkrafttreten für Kritik gesorgt, wurde aber auch aus Datenschutzkreisen zum Teil durchaus positiv begrüßt.[9] Fraglich erscheint daher ein weiteres Mal, ob der Beschluss aus den vorangegangenen Entscheidungen vor dem EuGH „gelernt hat“ oder ob nicht doch ein „Schrems III“ droht.[10]

1. Inhalt

Nach dem DPF können sich Unternehmen nach den sog. EU-US Data Privacy Principles selbst zertifizieren. Ähnlich wie schon

5 EuGH, Urt. v. 6.10.2015, C-362/14, Schrems; hierzu schon Sydow, Kein sicherer Hafen für die Daten?, DFN-Infobrief Recht 12/2015.

6 EuGH, Urt. v. 16.7.2020, C-311/18, Schrems II; hierzu Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

7 Hierzu z.B. Tiessen, Alles in der Schwebe, DFN-Infobrief Recht 4/2021; John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022.

8 Abrufbar unter: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf (zuletzt abgerufen am 15.9.2023).

9 Hierzu Tech, Kurzbeitrag: Data Privacy Framework – Die nächste Vollschremsung?, DFN-Infobrief Recht 5/2023; Palenberg, Auf die Schremse treten?, DFN-Infobrief Recht 2/2023; Mc Grath, Ausgeschremst?, DFN-Infobrief Recht 5/2022.

10 So schon die Ankündigung von noyb, der NGO von Max Schrems, abrufbar unter https://noyb.eu/de/european-commission-gives-eu-us-data-transfers-third-round-cjeu (zuletzt abgerufen am 15.9.2023).

unter Safe-Harbour und dem Privacy Shield enthält das DPF Datenschutzprinzipien, welche sich an der DSGVO orientieren. Diese sind von den selbstzertifizierten Unternehmen einzuhalten.[11] Das entspricht der Vorstellung der DSGVO, wonach die Schutzbedingungen für selbstzertifizierte Unternehmen ein angemessenes Niveau zu erreichen haben, das mit der DSGVO vergleichbar ist.[12] Dabei dürfen sich die Datenschutzregeln von der DSGVO unterscheiden, solange sie ein gleichwertiges Ergebnis erzielen.

Diese DPF Datenschutzprinzipen ähneln den vorherigen Privacy Shield Principles und Safe Harbor Principles. Dass an dieser Art der Regelung keine Änderung vorgenommen wird, liegt in der Entscheidung des EuGHs. Denn dieser hatte bislang nicht explizit über die Prinzipien geurteilt, sondern allgemein festgestellt, dass ein Selbstzertifizierungsmechanismus ein angemessenes Datenschutzniveau begründen könne. Das DPF kann als vereinfachte Version der DSGVO betrachtet werden, die wirtschaftsfreundlicher ausgestaltet ist. Es gibt beispielsweise Unterschiede bei der Weitergabe von Daten, der Auskunftspflichten und den Einwilligungsvoraussetzungen.

Eine weitere nennenswerte Änderung ist, dass US-Geheimdienste künftig nur auf Daten von Europäischen Bürger:innen zugreifen dürfen, wenn dies notwendig und verhältnismäßig ist. Bei der Entscheidung, ob die Verletzung der individuellen Rechte gerechtfertigt ist, müssen die Interessen der nationalen Sicherheit mit den Rechten der betroffenen Personen abgewogen werden. Dabei soll das Recht unparteiisch angewendet werden und die Entscheidungen der Amtsträger angemessen berücksichtigt werden.

Wie allerdings schon im Rahmen von Schrems II ist auch beim DPF kritisch zu betrachten, ob der vom neuen Framework gebotene Schutz vor rechtsstaatswidrigen behördlichen Zugriffen ausreichend ist. Hierfür hatte US-Präsident Biden im Vorfeld als Vorbereitung auf das DPF eine neue Executive Order (EO 14086) verabschiedet.[13] Der Unterschied zur zuvor geltenden Presidential Policy Directive (PPD-28), der Grundlage des Privacy Shields, ist vor allem die Einrichtung eines unabhängigen Gerichts zur Überprüfung des Datenschutzes. Dieses soll den vom EuGH kritisierten Ombudsmechanismus des Privacy Shields ersetzen. Für den EuGH genügte dieser Mechanismus nicht, weil er von der US-Regierung nicht unabhängig genug war und EU-Bürger:innen keine wirksamen Möglichkeiten zur Abhilfe im Falle einer Rechtsverletzung bot.[14]

In Bezug auf das neue DPF behauptet die EU-Kommission nun, dass die Änderungen diese Bedenken des EuGHs ausräumen. Das Rechtsschutzverfahren aus der EO 14086 sieht einen zweistufigen Rechtsschutzmechanismus vor. In der ersten Stufe reichen Beschwerdeführer ihre Beschwerden bei den Datenschutzbehörden ihres Heimatstaats ein, die sie an die US-Regierung weiterleiten.[15] Der Datenschutzbeauftragte der US-Geheimdienstkoordinationsstelle (Civil Liberties and Privacy Office (CLPO) bearbeitet die Beschwerde anstelle einer Ombudsperson im US-Außenministerium.[16] Die Entscheidung des Datenschutzbeauftragten ist bindend für die US-Geheimdienste, aber die Ergebnisse und Gründe werden nicht offengelegt.[17]

In der zweiten Stufe können Beschwerdeführer, ohne das Ergebnis der ersten Stufe zu kennen, Berufung beim Data Protection Review Court (DPRC) einlegen. Dieses Gremium, das unabhängig arbeiten soll und aus nicht-regierungsangehörigen Personen besteht,[18] prüft die Entscheidung des Datenschutzbeauftragten[19]

11 2.1.1 DPF

12 Art. 45 Abs. 1 S. 1 DSGVO; ErwG 104 S. 3 DSGVO.

13 Hierzu schon Palenberg, Auf die Schremse treten?, DFN-Infobrief Recht 2/2023.

14 Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 8/2020.

15 EO 14086, Sec. 3(b).

16 EO 14086, Sec. 3(c)(i).

17 EO 14086, Sec. 3(c)(i)(ii)(E)(1).

18 EO 14086, Sec. 3(d)(i)(A).

19 EO 14086, Sec. 3(d)(i)(D), (E).

und kann zusätzliche Informationen von den US-Geheimdiensten anfordern.[20] Die Beschwerdeführer werden von staatlich bestellten Sonderbeauftragten vor diesem Gericht vertreten.[21] Die Entscheidung des DPRC bleibt ebenfalls geheim.[22]

2. Kritik

Kritik erfährt das DPF vor allem hinsichtlich seiner Übereinstimmungen mit dem Privacy Shield. So bezeichnet noyb es als „weitgehende Kopie" und kritisiert, dass anders als behauptet nur wenig Änderungen im US-Recht erreicht werden. Die Kommission hätte bei der Ausarbeitung in die „Trickkiste" gegriffen und nur scheinbar Probleme gelöst.

Aber auch von Seiten der Aufsichtsbehörden wird Kritik geübt. Etwa übte die Aufsichtsbehörde in Baden-Württemberg Kritik an der Executive Order und zweifelte an, dass das Rechtsinstrument einer Executive Order überhaupt geeignet sei. Zudem monierte die Behörde, dass nicht klar sei, ob die US-amerikanische Auffassung von „verhältnismäßig" durch US-Geheimdienste mit dem europäischen Begriff der „Verhältnismäßigkeit" gleichgesetzt werden kann.[23] Der Kritik treten offen andere Aufsichtsbehörden entgegen, die sich vermittelnd für eine ergebnisoffene Prüfung aussprechen. Die Hamburger Aufsichtsbehörde, sieht in der Executive Order ein erprobtes Rechtsinstrument. Zum Kritikpunkt der „Verhältnismäßigkeit" wird angeführt, dass eine identische Auffassung grundsätzlich nicht zwangsläufig sei, da nur ein gleiches Niveau gefordert wäre.[24]

Tatsächlich ist fraglich, ob der EuGH das DPF in der Überprüfung wie auch seine Vorgänger für unwirksam erklärt. Denn die Kritikpunkte sind nicht unberechtigt. So ist der anzulegende Maßstab bei der Auslegung der Rechtsbegriffe zwischen den USA und der EU ein unterschiedlicher. Im EU-Recht wird darauf abgestellt, was notwendig und angemessen ist und im US-Recht hingegen, dass die Maßnahmen so begrenzt sein sollen, wie es machbar ist. Ob der EuGH diese Unterschiede angreift, wird maßgeblich vom hieraus resultierenden Schutzniveau in den USA abhängen. Auch die Unabhängigkeit der für das Beschwerdeverfahren vorgesehenen Gremien muss hinterfragt werden. Denn das CLPO gehört zum US-Geheimdienst, die Unabhängigkeit zur US-Regierung ist an dieser Stelle offensichtlich nicht gewahrt. Hinsichtlich des DPRC kann die Unabhängigkeit diskutiert werden, immerhin wird es durch regierungsunabhängige Personen besetzt. Allerdings verlangt Art. 47 Europäische Charta der Grundrechte (GRCh), welchen der EuGH als Voraussetzung sieht, ein „Gericht". Ob der DPRC als quasigerichtliches Verwaltungsgremium diesen Anforderungen genügt, ist offen. Zumindest verlangt die DSGVO nur ein der Sache nach gleichwertiges Schutzniveau, soweit der DPRC das Schutzniveau sicherstellen kann, kann das Gremium genügen.

Allerdings muss den Bürger:innen der EU für ein gleichwertiges Schutzniveau ein sog. faires und öffentliches Verfahren geboten werden. In der juristischen Literatur wird daher zu Recht in Frage gestellt, ob das Verfahren vor dem DPRC diesen Anforderungen genügen kann. Weder werden die beschwerdeführenden Personen am größten Teil des Verfahrens beteiligt, noch werden die Entscheidung und ihre Gründe vom DPRC öffentlich mittgeteilt. Dies entspricht nicht den Anforderungen der GRCh an ein faires und öffentliches Verfahren.

IV. Bedeutung für Hochschulen und Forschungseinrichtungen

Im Rahmen der Verwendung von Software, welche personenbezogene Daten in die USA übermittelt, kann sich jetzt prinzipiell wieder auf den Angemessenheitsbeschluss der Kommission gestützt werden. Einerseits vereinfacht das die Vertragslage, da nicht mehr auf die Standarddatenschutzklauseln (SCC) zurückgegriffen werden muss.[25] Doch der vermeintlich einfache Weg steht, wie oben aufgezeigt, unter keinem guten

20 EO 14086, Sec. 3(d)(ii).

21 EO 14086, Sec. 3(d)(i)(C).

22 EO 14086, Sec. 3(d)(i)(H).

23 LfDI, Pressemitteilung v. 26.10.2022, https://www.baden-wuerttemberg.datenschutz.de/usa-eu-datentransfer-durchfuehrungsverordnung-us-praesident/ (zuletzt abgerufen am 15.9.2023).

24 HmbBfDI, Mitteilung v. 29.11.2022, abrufbar unter https://datenschutz-hamburg.de/pages/executiveorder/ (zuletzt abgerufen am 15.9.2023).

25 Hierzu John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022; Tiessen, Santa Claus(e) is coming early, DFN-Infobrief Recht 8/2021; Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

Stern. Schon jetzt zeigen die Diskussionen um das DPF, dass auch diesem Angemessenheitsbeschluss möglicherweise die Nichtigkeit bevorsteht.

Denn nicht nur Schrems und sein Team beabsichtigten eine Klage gegen das DPF, sondern der französische Parlamentarier Phillippe Latombe hat jüngst im Wege eines Eilrechtsschutzes einen umfangreichen Schriftsatz beim EuGH eingereicht.[26] Darin macht er geltend, dass das DPF gegen eine Vielzahl an europäischen Normen verstößt. Ziel seiner Klage ist die sofortige Aussetzung der Gültigkeit des DPF bis zur Klärung, ob dieses inhaltlich mit den Unionsrechten vereinbar ist.

Allerdings wird bis zu einer Entscheidung des EuGHs noch etwas Zeit vergehen. Eine unmittelbare Auswirkung hat die Klageeinreichung auf die Wirksamkeit des DPF noch nicht. Auch Max Schrems und sein Team von nyob werden voraussichtlich für die angekündigte Anfechtung den Rechtsweg bei diesem Angemessenheitsbeschluss wieder von ganz unten beschreiten. Dennoch sollte gerade bei zentralen Softwareanwendungen stets äußerst sorgfältig abgewogen werden, ob man sich für erforderliche Datenexporte in die USA auf das DPF verlassen möchte. In die Abwägung sollten datenschutzfreundlichere Lösungen einbezogen oder die Möglichkeit der Rechtfertigung von Datenexporten anhand der vom EuGH nicht beanstandeten SCCs beleuchtet werden.

In jedem Fall kann man nicht davon ausgehen, dass das EU-US Data Privacy Framework die rechtliche Lage um Datenexporte in die USA gesichert hat. Erst die Bewertung des EuGHs wird hierzu Klarheit schaffen können.

26 Siehe Pressemitteilung von Latombe, https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf (zuletzt abgerufen am 15.9.2023).

Kurzbeitrag: Was kratzt mich das?

OLG Hamm: Scraping-Vorfälle bei Facebook rechtfertigen keinen DSGVO-Schadensersatz

von Ole-Christian Tech

Das Oberlandesgericht Hamm hat jüngst ein Leiturteil zu den sogenannten Facebook-Scraping-Fällen gesprochen (OLG Hamm, Urteil vom 15. August 2023, Az. 7 U 19/23).

Scraping, oft auch Web Scraping oder Screen Scraping genannt, bezeichnet eine Praxis, bei der mittels Programmen Informationen von Webseiten ausgelesen und somit bildlich gesprochen „geschürft" werden.

I. Was ist geschehen?

Im Verfahren vor dem OLG Hamm ging es darum, dass im April 2021 unbekannte Personen personenbezogene Daten von etwa 500 Millionen Facebook- Nutzern im Darknet veröffentlicht haben. Die Daten hatten die Unbekannten dabei unter Ausnutzung einer damaligen Suchfunktion von Facebook selbst gesammelt, weshalb hier von „Scraping" gesprochen wird. Diese Suchfunktion wurde zwar im Nachhinein durch Facebook deaktiviert, in Hinblick auf dieses Datenleck sind jedoch -nach der Entscheidung des Europäischen Gerichtshofs zu Grundsätzen des immateriellen Schadenersatzes (EuGH, Urteil vom 4. Mai 2023, Rs. C-300/21)[1] - eine Vielzahl von Klagen gegen Meta als Betreiberin der Plattform anhängig.[2]

Ursache des Rechtsstreits war die Suchfunktion bei Facebook, über die Personen durch die Suche nach ihrer Telefonnummer auffindbar waren. Selbst wenn die Betroffenen ihre Telefonnummer dabei nicht in ihrem Profil als sichtbar eingestellt hatten, wurde bei der Eingabe der Nummer in die Suchleiste das entsprechende Profil angezeigt. Die „Scraper" programmierten einen Code, der millionenfach Telefonnummern generierte und bei einem Treffer in der Suchleiste die Namen und sonstigen im Facebook-Profil hinterlegten Daten speicherte.

Nachdem Facebook auf diese Datenschutzlücke aufmerksam wurde, deaktivierte es die Funktion im April 2018. In der Folge stellten die Scraper ihre Methode um und nutzten diesmal die Kontaktimportfunktion, um weitere Daten zu schürfen. Hierauf reagierte Facebook dann für die Plattform im Oktober 2018 und für den Facebook-Messenger im September 2019.

II. Das Urteil

In der Urteilsbegründung erklärte das OLG Hamm nun, dass die Verarbeitung der personenbezogenen Daten der Betroffenen -namentlich der Telefonnummer- nicht auf Vertragszweckerfüllung gestützt werden kann und damit nicht nach Art. 6 Abs. 1 Unterabsatz 1 lit. b DSGVO gerechtfertigt war.
Weiterhin konnte auch ein etwaiges berechtigtes Interesse seitens Facebook an der Verarbeitung diese nicht nach Art. 6 Abs. 1 lit. f DSGVO rechtfertigen. Hierfür bedarf es grundsätzlich drei kumulativer Voraussetzungen:

1. Erstens muss von dem für die Verarbeitung Verantwortlichen oder von einem Dritten ein berechtigtes Interesse wahrgenommen werden,
2. zweitens muss die Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses

1 Hierzu vertiefend Voget, Nicht (un)erheblich?!, DFN-Infobrief Recht 07/2023.

2 Die erstinstanzliche Rechtsprechung ist hierzu noch uneinheitlich, ablehnend etwa Landgericht Bielefeld, Urteil vom 19. Dezember 2022, Az . 8 O 157/22, einen Anspruch bejahend dagegen LG Stuttgart, Urteil v. 26. Januar.2023, Az.: 530 95/22.

erforderlich sein und

3. drittens dürfen die Interessen oder Grundrechte und Grundfreiheiten der Person, deren Daten geschützt werden sollen, gegenüber dem berechtigten Interesse des Verantwortlichen oder eines Dritten nicht überwiegen.[3]

Das Gericht sah es bereits nicht als erforderlich an, diese Art der Rückwärtssuche zu ermöglichen, insbesondere da diese ja ohne Weiteres im April 2018 abgestellt werden konnte.
Zwar von Facebook nicht vorgetragen, vom Gericht aber dennoch beantwortet, wurde die Frage einer rechtfertigenden Einwilligung durch die Betroffenen nach Art. 5 Abs.1 lit. a Var. 1, Art. 6 Abs. 1 Unterabsatz 1 lit. a DSGVO.
Eine wirksame Einwilligung der Betroffenen in die Suchbarkeit ihres Nutzerprofils über die Mobilfunktelefonnummer lag allerdings in den Augen des Gerichts auch nicht vor, sodass mangels Rechtsgrundlage für die Verarbeitung dieser personenbezogenen Daten diese rechtwidrig war (sog. „Verbot mit Erlaubnisvorbehalt").

III. Unerlaubte Handlung, aber kein Schaden

Trotz dieser klaren datenschutzrechtlichen Einordnung des OLG Hamm wurde die Berufung der Klägerin zurückgewiesen, die Betroffene hat also verloren. „Die zulässige Leistungsklage ist aber unbegründet. Die Klägerin hat keinen Anspruch auf Ersatz eines immateriellen Schadens."[4] Aber warum?

Materiell-rechtlich handelt es sich bei dem Begehren der Klägerin um einen Anspruch auf Schadenersatz wegen unerlaubter Handlung (hier Art. 82 Abs. 1 DSGVO). Dieser setzt jedoch voraus, dass der Anspruchsgegner nicht nur gegen die DSGVO verstoßen hat- dies ist nach der Auffassung des OLG Hamm unstreitig- sondern auch, dass dem Anspruchssteller hierdurch kausal ein materieller oder immaterieller Schaden entstanden ist.
Materielle Schäden sind dabei Vermögensschäden, also solche, die in Geld bezifferbar und nicht der Persönlichkeitssphäre zuzuordnen sind. Dahingegen sind immaterielle Schäden jene unfreiwilligen Nachteile, die außerhalb von Vermögensdispositionen stehen und subjektiver Natur sind. Ein konkretes Beispiel hierfür wären etwa Schmerzen, der Ersatz dieser das Schmerzensgeld.[5]
Bereits nach dem Urteil des EuGHs zum Ersatz immaterieller Schäden wurde in der Literatur kontrovers diskutiert, inwieweit subjektive Empfindungen wie Ärger oder Verunsicherung ausreichen, um die Ersatzfähigkeit des immateriellen Schadens zu begründen.

Das Gericht führte hierzu aus: „Es entspricht indes schon nicht der allgemeinen Lebenserfahrung, dass das öffentliche Bekanntwerden der eigenen Mobilfunktelefonnummer, auch wenn es ungewollt erfolgt ist, regelmäßig / erfahrungsgemäß zu persönlichen / psychologischen Beeinträchtigungen führt."
Zwar ist das Risiko nicht unerheblich, da persönliche Informationen wie E-Mail-Adressen und Telefonnummern häufig zur Authentifizierung genutzt werden und somit auch von Kriminellen für Impersonation- also beispielsweise falsche Auskunftsansprüche nach Art. 15 DSGVO- genutzt werden können und somit immer weitere sensiblere Informationen erlangen können (sog. Daisy Chains).[6]
Dem OLG Hamm kam es jedoch vor allem auf den Vortrag der Klägerin an, welche lediglich ausgeführt hatte, ein „Gefühl der Erschrockenheit" erlitten zu haben. Dies reichte dem OLG nicht aus.

IV. Folgen für Wissenschaft und Forschung

Für datenverarbeitende Stellen wie Hochschulen und Forschungseinrichtungen zeigt auch dieses Urteil wieder auf, wie wichtig die Grundlagen zu datenschutzfreundlicher Grundeinstellung („privacy by default") und datenschutzfreundlicher Technologie („privacy by design") sind, um ungewollte rechtsgrundlagenlose Verarbeitung personenbezogener Daten zu vermeiden. Die neueren Methoden des Web Scraping werfen einmal mehr ein Schlaglicht auf die Praxis, die den DSGVO Compliance Anforderungen hier noch nicht hinreichend nachgekommen ist.

---

3 OLG Hamm, Urteil vom 15. August 2023, Az. 7 U 19/23 Rz. 109.

4 OLG Hamm, Urteil vom 15. August 2023, Az. 7 U 19/23 Rz. 57.

5 Hierzu bereits Müller, Morgen Kinder werden wir klagen, DFN-Infobrief Recht 12/2022 und selbiger in Schaden oder kein Schaden, das ist hier die Frage, DFN-Infobrief Recht 03/2023.

6 Hierzu vertiefend Tech, Doppelgänger Delights: How to prevent the perfect impersonation (Or Not), DFN-Infobrief Recht 04/2023.

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