DFN infobrief recht

4 / 2022
April 2022

Machtwort gegen Hass und Hetze

Das Bundesverfassungsgericht zu Hetzkommentaren auf Facebook und dem allgemeinen Persönlichkeitsrecht

Wer einen Account stiehlt, stiehlt auch ein Kamel

LG Essen zu Rechten an Social-Media Accounts

Data Wars: Episode IV - Eine neue Richtung

Die Regierung von Boris Johnson legt im Vereinigten Königreich einen Vorschlag zur Reformierung des britischen Datenschutzrechts vor

Machtwort gegen Hass und Hetze

Das Bundesverfassungsgericht zu Hetzkommentaren auf Facebook und dem allgemeinen Persönlichkeitsrecht

von Johanna Schaller

Das oberste Gericht setzt in seinem Beschluss neue Maßstäbe für herabsetzende Kommentare im Netz und hebt die Entscheidungen des Landgerichts (LG) und Kammergerichts (KG) Berlin auf. Auch der Schutz der Persönlichkeitsrechte von Amtsträger:innen und Politiker:innen wird durch diese Entscheidung gestärkt. Dabei handelt es sich jedoch zunächst nur um einen Zwischenerfolg: Das KG Berlin muss sich nun erneut mit den einzelnen Kommentaren auseinandersetzen und eine ausführliche Abwägung vornehmen.

I. Was bisher geschah

Die Grünen-Politikerin Renate Künast führt seit 2019 einen Rechtsstreit vor dem Landgericht und Kammergericht in Berlin. Dabei geht es um Nutzerkommentare auf dem sozialen Netzwerk Facebook, die unter einer falsch zitierten Äußerung Künasts abgegeben wurden. Unter anderem verwendeten die Nutzer:innen Ausdrücke wie „Schlampe“, „Pädophilen-Trulla“ und „gehirnamputiert“.
Künast beansprucht von Facebook Auskunft der Nutzerdaten von 22 Kommentator:innen.

Der Plattformbetreiber muss grundsätzlich die Anonymität seiner Nutzer:innen schützen. Eine Auskunft kann daher nur im Ausnahmefall gewährt werden. Eine solche Ausnahmebefreiung des Plattformbetreibers von seinen datenschutzrechtlichen Pflichten sieht der im Zeitpunkt des Streitfalls geltende § 14 Abs. 3 Telemediengesetz (TMG) a.F., bzw. nunmehr § 21 Abs. 2 und 3 Telekommunikation-Telemedien-Datenschutz-Gesetze (TTDSG) iVm § 1 Abs. 3 Netzwerkdurchsetzungsgesetz (NetzDG) vor.[1] Der Anspruch auf Auskunftserteilung besteht danach, wenn die Äußerungen rechtswidrig sind und der Betroffene durch die rechtswidrigen Inhalte in seinen absoluten Rechten verletzt wird. Dazu nennt § 1 Abs. 3 NetzDG die in Betracht kommenden Straftatbestände, unter anderem die Beleidigung gem. § 185 Strafgesetzbuch (StGB). Für die Freigabe der Auskunftserteilung, die der Durchsetzung der Ansprüche gegen die Nutzer:innen auf Unterlassen der ehrbeeinträchtigenden Äußerungen dient, ist eine gerichtliche Feststellung erforderlich. Das Landgericht Berlin erkannte in seiner ersten Entscheidung (Beschluss vom 9.9.2019 – 27 AR 17/19) in den gegenständlichen Kommentaren zunächst keine Diffamierungen und Beleidigungen. Nach einer Beschwerde Künasts änderte es seine Entscheidung im Abhilfeverfahren nur teilweise ab (Beschluss vom 21.1.2020 – 27 AR 17/19). In der nächsten Instanz gab das Kammergericht (Beschluss vom 11.3.2020 – 10 W 13/20) sodann zwar in weiterem Umfang der Klage der Politikerin statt, indem es weitere 6 Äußerungen als unzulässig einstufte und diesbezüglich die Herausgabe der Nutzerdaten bewilligte, hinsichtlich der verbleibenden 10 Kommentare entsprach es der Klage Künasts jedoch nicht. Die Anhörungsrüge der Politikerin wies das Kammergericht anschließend mit Beschluss vom 06.04.2020 zurück. Gegen die Entscheidungen legte Renate Künast Verfassungsbeschwerde vor dem Bundesverfassungsgericht (BVerfG) ein.

II.Das Machtwort des BVerfG

Eingangs ist festzuhalten, dass das BVerfG keine sogenannte „Superrevisionsinstanz“ ist. Das bedeutet, dass eine Verwerfungskompetenz des BVerfG bei Urteilsverfassungsbeschwerden nur bei besonderen Fehlern, nämlich dem Verstoß gegen

1 Tiessen, Sag mir deinen Namen und ich sag dir, was du bist – LG Berlin zu Auskunftsansprüchen wegen Beleidigung auf Social Media-Plattformen, DFN-Infobrief Recht 5/2020, S. 2.

Verfassungsrecht gegeben ist. Das BVerfG korrigiert angegriffene Urteile daher erst dann, wenn die gerichtliche Entscheidung Auslegungsfehler erkennen lässt, die auf einer grundsätzlich unrichtigen Auffassung von der Bedeutung und Tragweite der Grundrechte, insbesondere bezüglich des Umfangs der Schutzbereiche der Grundrechte beruht.
Einen solchen Fall bejaht das oberste Gericht hier. Ausgangspunkt für den Verstoß gegen Verfassungsrecht ist nach Auffassung des BVerfG der Umstand, dass das KG eine Schmähung mit der Beleidigung i.S.d. § 185 StGB gleichsetze. Grundsätzlich obliege die Auslegung und Anwendung der einschlägigen Bestimmungen des TMG und der in Verweis genommenen Vorschriften, so hier das Strafgesetzbuch, den ordentlichen Gerichten. Dabei müsse der Spruchkörper die betroffenen Grundrechte interpretationsleitend berücksichtigen, damit deren wertsetzender Gehalt auch auf der Rechtsanwendungsebene gewahrt bleibt. An dieser Stelle nimmt das BVerfG eine ausführliche Skizzierung der Auslegung des § 185 StGB und der Prüfung, ob eine strafbare Beleidigung vorliegt, vor:

Zunächst sei der Inhalt der verfahrensgegenständlichen Äußerung zu ermitteln und festzustellen, ob der Kommentar nach seinem objektiven Sinngehalt das Persönlichkeitsrecht des Betroffenen beeinträchtigt.

In einem zweiten Schritt sei sodann eine abwägende Gewichtung der Beeinträchtigungen, die den betroffenen Rechtsgütern und Interessen, also der Meinungsfreiheit und der persönlichen Ehre drohen, vorzunehmen. Eine solche Abwägung sei nur ausnahmsweise entbehrlich, wenn die streitgegenständlichen Äußerungen sich als Schmähung oder Schmähkritik, Formalbeleidigung oder Angriff auf die Menschenwürde darstellen. Eine Schmähung im verfassungsrechtlichen Sinne liege dann vor, wenn eine Äußerung keinen irgendwie nachvollziehbaren Bezug mehr zu einer sachlichen Auseinandersetzung hat und es bei ihr im Grunde nur um das Verächtlichmachen der betroffenen Person als solcher geht.
Liegt kein Fall der Schmähung vor, stelle dies kein Indiz für eine Straflosigkeit und einen Vorrang der Meinungsfreiheit dar. Vielmehr müsse dann die erforderliche Abwägung vorgenommen werden, die an den wertungsoffenen Merkmalen des Beleidigungstatbestandes, „Beleidigung", „Wahrnehmung berechtigter Interessen" anknüpft. Erforderlich sei an dieser Stelle eine umfassende Auseinandersetzung mit den konkreten Umständen des Falles und der Situation, in der die Äußerung erfolgte.

Als maßgebliche Abwägungskriterien kristallisiert das BVerfG folgende heraus: Zunächst sei das Gewicht der Meinungsfreiheit höher anzusetzen, wenn die Äußerung einen Beitrag zur öffentlichen Meinungsbildung bezweckt. Dementsprechend geringer sei das Gewicht bei einer „emotionalisierenden Verbreitung von Stimmungen gegen einzelne Personen".

Des Weiteren sei zu berücksichtigen, dass die Grenzen zulässiger Kritik bei Amtsträger:innen weiter auszulegen seien. Die Meinungsfreiheit sei hier besonders schutzwürdig. Diese Auffassung werde gestützt durch die Auslegung und Anwendung von Art. 10 Abs. 2 Europäische Menschenrechtskonvention (EMRK), insbesondere durch die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte (EGMR). Aber auch im Falle der sog. „Machtkritik" gelte: Äußerungen seien weniger schutzwürdig, je mehr die Herabwürdigung einer Person in den Vordergrund tritt.

Überdies sei auch relevant, ob die Äußerungen spontan gefallen seien oder mit längerem Vorbedacht getätigt wurden. Das oberste Gericht nimmt hier eine rechtliche Anerkennung der Grenzen zumutbarer Selbstbeherrschung vor. Es geht davon aus, dass bei schriftlichen Äußerungen, also auch bei textlichen Äußerungen in sozialen Netzwerken, ein höheres Maß an Bedacht und Zurückhaltung zu erwarten sei.

Zuletzt sei auch die Breitenwirkung der Äußerung ein maßgeblich in die Abwägung einzustellendes Kriterium. Die beeinträchtigende Wirkung sei höher, wenn sie besonders sichtbar in einem der allgemeinen Öffentlichkeit zugänglichen Medium, wie hier ein soziales Netzwerk im Internet, getätigt wird.

Die Entscheidung des KG genüge diesen Anforderungen nicht und lege wiederholt einen fehlerhaften, mit dem Persönlichkeitsrecht unvereinbar hohen Maßstab an eine Rechtsverletzung an. Konkret lastet das oberste Gericht dem KG an, es verkenne die verfassungsrechtlichen Voraussetzungen des Beleidigungstatbestandes, indem es davon ausgehe, dass der Tatbestand der Beleidigung nur im Fall einer Schmähung vorliege. Vielmehr müsse aber, wenn der Sonderfall der Schmähung nicht vorliege, eine Abwägung vorgenommen werden. Im Falle des Überwiegens der Persönlichkeitsrechtsverletzung, sei sodann auch der Tatbestand der Beleidigung erfüllt.

Der Entscheidung kommt grundsätzliche Bedeutung zu, da das Verfassungsgericht anerkennt, dass der Schutz der

Persönlichkeitsrechte von Amtsträger:innen auch im öffentlichen Interesse ist. Die Bereitschaft der Amtsträger:innen, der Gesellschaft einen Dienst zu erweisen, sei in der Abwägung zugunsten der Betroffenen, also zugunsten des Persönlichkeitsrechts, zu berücksichtigen. In der Konsequenz hob das BVerfG die Beschlüsse des KGs auf und verwies den Rechtsstreit zur erneuten Entscheidung an selbiges zurück.

Die strafrechtliche Beurteilung der Erfüllung des Beleidigungstatbestandes und die damit verbundene Frage nach dem Bestehen eines Herausgabeanspruchs Künasts bezüglich der weiteren Nutzerdaten sind somit weiterhin offen. Schließlich ist es, wie das BVerfG in seiner Entscheidung betonte, Aufgabe der Fachgerichte aufgrund der Umstände des Einzelfalls die abwägungsrelevanten Gesichtspunkte herauszuarbeiten und diese unter Berücksichtigung der vom obersten Gericht aufgestellten Leitlinien gegeneinander abzuwägen.

Möglicherweise könnte in der nun anstehenden Entscheidung des KGs auch die Stolpe-Rechtsprechung des BVerfG (Beschluss vom 25.10.2005 – 1 BvR 1696/98) Berücksichtigung finden. Damals stellte das oberste Gericht fest, dass bei Vorliegen einer, das Persönlichkeitsrecht eines Anderen verletzenden, mehrdeutigen Meinungsäußerung ein Anspruch auf deren zukünftige Unterlassung nicht allein deshalb ausscheidet, weil auch eine Deutungsvariante möglich ist, die zu keiner Persönlichkeitsbeeinträchtigung führt.

Anders entschied das BVerfG bei einer in der Vergangenheit erfolgten mehrdeutigen Äußerung, die zur Verurteilung, etwa zu einer Strafe, zur Leistung von Schadensersatz oder zum Widerruf führte. Hier könne nicht die Deutungsvariante zugunsten der Persönlichkeitsrechtsverletzung angenommen werden, wenn auch eine Deutungsmöglichkeit bestehe, die zur Straflosigkeit führe (Beschluss vom 19.04.1990 – 1 BvR 40/86, Strauß-Transparent). Im Fall Renate Künast könnte eine Mehrdeutigkeit bei einigen Äußerungen angenommen werden. Nach der BVerfG Rechtsprechung wären dann aber jedenfalls die Voraussetzungen eines Unterlassungsanspruchs erfüllt.

III. Fazit / Bedeutung für Hochschulen

In Zeiten der Corona-Pandemie ist das Arbeiten und der Austausch auf digitalen Plattformen relevanter denn je. Unter dem Deckmantel der Anonymität und einer herabgesetzten Hemmschwelle mangels persönlicher, unmittelbarer Konfrontation werden die Netzwerke zunehmend zur Stimmungsmache und Verbreitung von Hass, Wut oder sexuellen Übergriffen missbraucht.

Die Problematik der ungehemmten digitalen Kommunikation betrifft auch die Hochschulen.[2] Dies zeigte bereits der Fall aus dem Jahr 2015 an der Universität Göttingen: Eine Dozentin wurde über die App Jodel von mehreren Studierenden anonym sexuell belästigt. Ebenfalls im Jahr 2015 streuten anonyme Gruppen und Nutzer:innen im Netz Gerüchte über Hochschulprofessoren der Humboldt-Universität Berlin.[3] Ihnen wurde dort vorgeworfen, Rassisten, Faschisten und/oder Kolonialverbrecher zu sein. Auch in der Politik zeitigt die Hetze im Netz ihre Folgen: Nach Robert Habeck hat nun auch Schleswig-Holsteins Bildungsministerin Karin Prien (CDU) ihre Twitter-Präsenz auf Eis gelegt.

Soziale Medien werden in der heutigen Gesellschaft nicht nur zum Vernetzen, sondern ebenso zur Informationsbeschaffung und Meinungsäußerung genutzt. Klare Leitlinien, um der Entwicklung hin zu einer Verrohung der Kommunikation und des Umgangs miteinander und der Verbreitung von Hassbotschaften entgegen zu wirken, sind daher begrüßenswert, wenn nicht sogar unverzichtbar.

2 Tiessen, Sag mir deinen Namen und ich sag dir, was du bist – LG Berlin zu Auskunftsansprüchen wegen Beleidigung auf Social Media-Plattformen, DFN-Infobrief Recht 5/2020, S. 4.

3 Röttgen, Die Gedanken sind frei – Worte nicht unbedingt, DFN-Infobrief 2/2018, S. 1 ff.

Wer einen Account stiehlt, stiehlt auch ein Kamel

Landgericht Essen zu Rechten an Social-Media Accounts

von Justin Rennert

Social-Media Accounts sind heutzutage eine Selbstverständlichkeit. Auch für Hochschulen sind sie oft essentieller Bestandteil der Außendarstellung. Eine aktuelle Entscheidung des Landgerichts (LG) Essen zeigt, wie unklar die Rechtslage bezüglich der Rechte an Social-Media Accounts eigentlich ist. Grund genug, sich mit der Entscheidung selbst und den Rechten an Accounts im Allgemeinen näher zu beschäftigen.

I. Einleitung

Social-Media Accounts dienen schon lange nicht mehr nur der persönlichen Kommunikation zwischen Privatpersonen und dem Teilen von lustigen Hundefotos. Private Unternehmen, aber auch öffentliche Stellen wie Hochschulen nutzen sie zu ihren Zwecken. Dabei können die Accounts bei privatwirtschaftlichen Unternehmen sogar zum Dreh- und Angelpunkt der geschäftlichen Tätigkeit werden. Nur ein Beispiel hierfür liefert ein Fall, den jüngst das LG Essen zu entscheiden hatte: Die Klägerin hatte sich auf das Veranstalten von Turnieren und Ligaveranstaltungen im elektronischen Dartssport in Deutschland spezialisiert, die fast ausschließlich über eine Facebook-Seite organisiert wurden. Über die Facebook-Seite wurden die Termine für die Turniere bekanntgegeben, darüber hinaus fungierte die Seite als Treffpunkt der Spieler und Organisatoren. Die Facebook-Seite wurde von der Beklagten betrieben, die auch die sonstige Hard- und Software zum Betrieb der Dartsveranstaltungen bereitstellte und der Klägerin ein Administratorenrecht für den Facebook-Account eingeräumt hatte. Einige Monate später entzog die Beklagte die eingeräumten Administratorenrechte allerdings wieder, was die Durchführung von Darts-Tunieren für die Klägerin so sehr erschwerte, dass sie sich genötigt sah, gerichtlich gegen die Beklagte vorzugehen. Der Fall zeigt exemplarisch die heute häufig anzutreffende Abhängigkeit vom Betrieb von Social-Media-Accounts im Wirtschaftsverkehr. Er soll daher zum Anlass genommen werden, aufzuzeigen, welche Rechte an einem Account bestehen können. Damit zusammen hängt auch die Frage, welche Möglichkeiten der Inhaber eines Accounts hat, um sich gegen Übergriffe wie den obigen zur Wehr zu setzen.

II.Rechte an Accounts

Die Frage nach Rechten an Accounts hängt eng mit der Frage des Rechts an Daten zusammen. Diese Frage ist in der juristischen Literatur und Rechtsprechung heiß umkämpft und Gegenstand ständiger Debatten und Richtungswechsel. Im Zentrum der zivilrechtlichen Streitigkeiten steht § 90 BGB, der den zivilrechtlichen Sachbegriff normiert.[1] Demnach sind Sachen nur körperliche Gegenstände. Daten (so auch Account-Daten) fehlt aber grundsätzlich die hierfür erforderliche körperliche Abgrenzbarkeit. Dennoch gibt es zahlreiche Lösungsvorschläge dahingehend, Daten doch im Sinne eines Dateneigentums oder Datenbesitzes eindeutig einer Person zuzuordnen. Mit der Anerkennung eines solchen Eigentums oder Besitzes an Daten gingen dann die Rechtsbehelfe einher, die das BGB zum Schutz des Eigentums und des Besitzes vorsieht. Solange Dateneigentum oder Datenbesitz nicht höchstrichterlich anerkannt sind, spielen diese Konstruktionen für die Praxis allerdings keine Rolle. Das bedeutet indes nicht,

1 Zu den strafrechtlichen Konsequenzen des Account-Hijackings: John, Error 403: Zugriff verweigert, DFN-Infobrief Recht 03/2021.

dass ihre Entwicklung nicht sorgsam verfolgt werden sollte. Sollte es zu maßgeblichen Neuerungen kommen, wird natürlich auch im DFN-Infobrief darüber informiert werden.
Auch heute sind aber schon zahlreiche mit einem Account zusammenhängende Rechte anerkannt, die im Einzelfall dem Inhaber eines Accounts Handlungsmöglichkeiten eröffnen.

An erster Stelle zu nennen sind vertragliche Rechte. Zwischen dem Plattformbetreiber und dem Account-Inhaber besteht ein Vertragsverhältnis kraft dessen sowohl dem Plattformbetreiber und dem Inhaber verschiedene Rechte zukommen können. Da Schuldverhältnisse stets nur relativ wirken, d.h. nur im Verhältnis zwischen den Vertragsparteien, kann sich der Account-Inhaber aber auch nur gegenüber dem Plattformbetreiber auf diesen Vertrag berufen. Bei Übergriffen Dritter hingegen hilft ihm sein Vertrag mit dem Plattformbetreiber nicht weiter. Der Account-Inhaber kann darüber hinaus aber auch Verträge bezüglich seines Accounts mit Dritten schließen. Er kann seinen Account z.B. verkaufen oder einem Dritten – wie im durch das LG Essen zu beurteilenden Fall – ein Administratorenrecht einräumen. Dann können sich wiederum der Account-Inhaber (Verkäufer) und der Käufer im Verhältnis zueinander auf den zwischen ihnen geschlossenen Vertrag berufen. Vertragliche Rechte können also immer nur dann relevant werden, wenn der Account-Inhaber zuvor ein vertragliches Verhältnis mit der anderen Partei eingegangen ist. Hiervon werden zwar schon viele Fälle abgedeckt, es sind aber mindestens genauso viele Fälle vorstellbar, in denen ein vertragliches Verhältnis gerade nicht besteht. So etwa, wenn ein Unbekannter Inhalte des Accounts unbefugt kopiert.

Aus diesem Grund stellt sich der Rechtswissenschaft die Frage nach absoluten Rechten des Account-Inhaber, d.h. solchen Rechten, die nicht nur gegenüber einem Vertragspartner gelten, sondern gegenüber jedermann. Die Antwort vorweg: Nach derzeitiger Rechtslage besteht an Daten grundsätzlich kein umfassendes absolutes Recht. Gesetzlich geregelt sind lediglich Teilbereiche. Hier müssen das Geschäftsgeheimnisrecht (geregelt im GeschGehG), das Datenbankherstellerrecht (§§ 87a ff. UrhG) und das Schutzrecht für Computerprogramme genannt werden (§§ 69a ff. UrhG). Diese Teilrechtsordnungen können im Einzelfall bewirken, dass Daten absolut oder nahezu absolut geschützt sind. Allerdings besteht der Schutz dann nicht für das Datum an sich und auch nicht allein wegen seiner Eigenschaft als Datum. Vielmehr verleihen die Teilrechtsordnungen den Schutz aus anderen Erwägungen. Das Geschäftsgeheimnisrecht schützt Informationen dann, wenn der Inhaber angemessene Geheimhaltungsmaßnahmen getroffen hat. Schutz besteht also für geschäftlich geheim gehaltenes Know-How, unabhängig davon, ob es sich dabei um Daten oder andere Informationen handelt.[2] Das Datenbankherstellerrecht besteht hingegen nicht für einzelne Daten, sondern nur für eine Datenbank als Gesamtheit. Schutz besteht zudem nur dann, wenn bei der Erstellung der Datenbank eine wesentliche Investition getätigt wurde. Anknüpfungspunkt für den Schutz ist also wiederum nicht die Dateneigenschaft als solche, sondern eine vorgelagerte Investition.

An dieser Stelle mag sich die Eine oder der Andere wundern und fragen: Ist der Schutz von Daten an sich nicht gerade Aufgabe des Datenschutzrechts? Der Name legt dies jedenfalls nahe. Allerdings verleiht das Datenschutzrecht ebenfalls kein absolutes, gegen jedermann wirkendes Recht. Es handelt sich wiederum nur um einen teilweisen Schutz. Dieser knüpft wiederum nicht an die Dateneigenschaft als solche, sondern an den Personenbezug von Daten an. Nicht personenbezogene Daten werden durch das Datenschutzrecht nicht geschützt.

Zurück zu dem Fall, den das LG Essen zu entscheiden hatte: Ging es hier nicht um einen Facebook-Account? Für einen Facebook-Account benötigt der Nutzer ein Passwort. Es handelt sich hierbei ja gerade um eine Information, die ihr Inhaber vor dem Zugriff anderer geheim hält. Ein Passwort kann durchaus nach dem Geschäftsgeheimnisrecht geschützt sein. Allerdings stritten die Parteien hier nicht um das Passwort, sondern um die Administratorenrechte für den Account. Dabei handelt es sich nicht um eine geheim gehaltene Information und somit ist der Geheimnisschutz hier nicht einschlägig.

Die Klägerin versuchte die Administratorenrechte somit auf anderem Wege zurück zu erlangen. Sie machte geltend, dass es sich bei dem Entzug der Rechte um verbotene Eigenmacht gehandelt habe. Verbote Eigenmacht ist ein Begriff aus dem allgemeinen Zivilrecht. Verbotene Eigenmacht kann grundsätzlich nur an Sachen verübt werden. Sachen sind nur körperliche Gegenstände. Daten, auch Account-Daten und Administratorenrechte, sind hingegen keine körperlichen Gegenstände, sondern unkörperlicher Natur. Sie existieren auf einer Festplatte oder einem sonstigen Datenträger, können

2 Vertiefend zur Frage, ob auch Forschungsdaten Geschäftsgeheimnisse sein können: Rennert, In geheimer Mission, DFN-Infobrief Recht 01/2022.

aber nicht räumlich erfasst und abgegrenzt werden. Mit dieser Begründung lehnte sodann auch das LG Essen den Anspruch der Klägerin ab. Auch eine entsprechende Anwendung der Vorschriften über die verbotene Eigenmacht komme nicht in Betracht. Körperliche Gegenstände zeichneten sich vor allem durch drei Eigenschaften aus: ihre Rivalität, Exklusivität und Abnutzbarkeit. Rivalität bedeutet, dass jeweils nur eine Person den Besitz an der Sache innehalten kann. Exklusivität meint, dass die Sache nicht kopierbar ist. Und Abnutzbarkeit meint, dass die Nutzung der Sache zu einem mehr oder weniger schnellen Verschleiß führt. All diese Eigenschaften seien für Daten nicht gegeben. Diese seien beliebig kopierbar, für mehrere Personen zeitgleich zugänglich und nicht abnutzbar.

Das letzte Wort ist in diesem Fall allerdings noch nicht gesprochen. Die Entscheidung des LG Essen erging in einem einstweiligen Verfügungsverfahren. Eine Entscheidung in der Hauptsache steht noch aus. Und das könnte durchaus spannend werden. Denn im Hauptsacheverfahren ist damit zu rechnen, dass die Klägerin auch die hier nur kurz angesprochenen Schutzrechte (insbesondere Geschäftsgeheimnisse) und vertraglichen Rechte geltend macht.

III. Fazit und Bedeutung für Hochschulen

Die Debatte um juristische Befugnisse an Accounts ist nicht erst seit gestern in vollem Gange. Zumindest für das Erbrecht hat der Bundesgerichtshof (BGH) im Jahr 2020 mit einer viel beachteten Entscheidung für Klarheit gesorgt. Der Entscheidung des BGH lag ein dramatischer Sachverhalt zugrunde: Ein noch minderjähriges Kind, das mit Zustimmung der Eltern einen Facebook-Account eröffnet hatte, verstarb. Die Eltern begehrten von Facebook den Zugang zu dem Account und den enthaltenen Kommunikationsinhalten, was Facebook ablehnte. Der daraufhin zwischen Facebook und den Eltern geführte Rechtsstreit drehte sich also um die Frage, ob der Facebook-Account des Kindes vererblich ist, mit anderen Worten ob er zum Nachlass des Kindes gehört. Während die erste Instanz den Eltern Recht gab, entschied das Berufungsgericht zugunsten von Facebook. Erst beim BGH konnten sich die Eltern endgültig durchsetzen. In seiner Entscheidung stellte der BGH zunächst grundlegend fest, dass der Nutzungsvertrag zwischen dem Kind und Facebook vererblich ist. Weiter führte er aus, dass der Vererblichkeit auch keine Persönlichkeitsrechte der Kommunikationspartner des Kindes, das Telekommunikations-, oder das Datenschutzrecht entgegenstehen. Mit anderen Worten entschied der BGH also, dass der Facebook-Account in vollem Umfang vererblich ist.[3] So klar ist die Rechtlage wie gesehen leider längst nicht überall. Dennoch lohnt sich die Auseinandersetzung mit der Materie auch für Hochschulen. Denn auch im öffentlichen Sektor hat es sich schon lange etabliert, Social-Media-Accounts zu betreiben. Diese werden nicht selten auch zur Informationsweitergabe an Mitarbeiter und Studierende genutzt und können eine zentrale Rolle in der Außendarstellung der Hochschule spielen. Um eine möglichst große Rechtssicherheit zu erreichen, sollten sich Hochschulen zunächst mit den Nutzungsverträgen zwischen ihnen und den Betreibern der Social-Media Plattformen auseinandersetzen. Das sollte bestenfalls immer schon vor Eröffnung eines Kontos geschehen. Gleiches gilt, wenn bezüglich der Social-Media-Accounts der Hochschule Verträge mit Dritten geschlossen werden. Hier liegt, wie der Fall des LG Essen zeigt, ein nicht zu unterschätzendes Potential für Streitigkeiten und Probleme. Klare vertragliche Regelungen können dem vorbeugen. Zuletzt sei angeraten, die rechtliche Entwicklung im Auge zu behalten. Neuerungen können sich auf Ebene der Rechtsprechung ergeben, aber auch durch ein Tätigwerden des Gesetzgebers. Sollte es hier zu einem Umbruch kommen, wird im DFN-Infobrief Recht natürlich darüber zu lesen sein.

3 Siehe zum Ganzen schon: Tiessen, Der lange Weg zum letzten Willen, DFN-Infobrief Recht 11/2020.

Data Wars: Episode IV - Eine neue Richtung

Die Regierung von Boris Johnson legt im Vereinigten Königreich einen Vorschlag zur Reformierung des britischen Datenschutzrechts vor

von Nicolas John

Der Austritt des Vereinigten Königreichs, der sog. „Brexit" hat viele Gesichter. So ändern sich nicht nur Reisebedingungen für Touristen und Geschäftsreisende oder Regulierungen für den Warenverkehr, sondern auch im Datenschutzrecht kommt Bewegung ins Spiel. So gilt bislang im Vereinigten Königreich eine nur leicht abgewandelte Version der Datenschutz-Grundverordnung (DSGVO), die UK General Data Protection Regulation (UK GDPR). Doch die Übernahme der Normen der DSGVO in das britische Recht stellt nur eine Übergangslösung dar. Nun ist ein Regierungspapier[1] veröffentlicht worden, welches weitreichende Änderungen im britischen Datenschutzrecht vorschlägt. Von den Regelungsvorschlägen sind auch Datenverarbeitungen zu Forschungszwecken betroffen.

I. Hintergrund

Formell gilt innerhalb des Vereinigten Königreichs seit dem Austritt aus der Europäischen Union das europäische Recht nicht mehr.[2] Doch aufgrund der knappen zeitlichen Umsetzung des Brexit konnte die britische Legislative viele Gesetze nicht neu entwerfen und übernahm daher zunächst große Teile europäischer Rechtsvorschriften, um Regelungslücken und damit verbundene Risiken zu vermeiden. Auch die DSGVO wurde mit nur wenigen Änderungen übernommen und fungiert seit dem Austritt als zentrales Datenschutzgesetz im Vereinigten Königreich. Hierdurch ähnelt das britische Datenschutzrecht weiterhin dem der Europäischen Union.

Dies ist für Datenverarbeitende im Geltungsbereich der europäischen DSGVO dann relevant, wenn sie Daten in das Vereinigte Königreich exportieren wollen. Denn Art. 45 Abs.1 DSGVO verlangt für den Export personenbezogener Daten in ein Drittland außerhalb des Geltungsbereichs der DSGVO, dass die Kommission festgestellt hat, dass das Drittland ein angemessenes Datenschutzniveau bietet. Wenn ein solcher Angemessenheitsbeschluss nicht vorliegt, ist ein Datenexport nur vorbehaltlich geeigneter Garantien, wie beispielsweise der Verwendung von Standarddatenschutzklauseln und entsprechender technischer und organisatorischer Maßnahmen, möglich.[3] Da ein Datenexport unter Bereitstellung dieser Garantien stets aufwändiger ist und ein angemessenes Datenschutzniveau in einem Drittland auch generell einen höheren Schutzstandard verspricht, ist der Export aufgrund eines Angemessenheitsbeschlusses nach Art. 45 DSGVO die bevorzugte Grundlage.

Im Rahmen der Prüfung, ob ein angemessenes Datenschutzniveau vorliegt, analysiert die Europäische Kommission einen umfangreichen Katalog an zu erfüllenden Faktoren. Untersucht wird zum Beispiel, ob die Rechtsstaatlichkeit oder die Menschenrechte und Grundfreiheiten geachtet werden, welche Rechtsvorschriften bezüglich personenbezogener Daten

1 Department for Digital, Culture Media & Sport, Data: A new direction, 10.09.2021, abrufbar unter https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf (zuletzt abgerufen am 17.2.2022).

2 Zu den datenschutzrechtlichen Auswirkungen des Brexit: Nickoleit, Der Tragödie letzter Teil?, DFN-Infobrief Recht 5/2021.

3 Zu den Standarddatenschutzklauseln: John, New Schrems, new Me(crosoft), DFN-Infobrief Recht 2/2022; Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

Anwendung finden und ob betroffenen Personen vergleichbar wirksame und durchsetzbare Rechte im Rahmen eines funktionierenden Rechtsbehelfsverfahrens im Drittland zur Verfügung stehen. Darüber hinaus werden beispielsweise auch das Vorhandensein und die wirksame Funktionsweise von Aufsichtsbehörden einschließlich entsprechender Durchsetzungsbefugnisse, sowie international eingegangene Verpflichtungen, welche die personenbezogenen Daten tangieren, von der Kommission beleuchtet.

Für die im Vereinigten Königreich derzeit geltenden Vorschriften der UK GDPR konnte die Europäische Kommission aufgrund der mehrheitlich übernommenen Normen der DSGVO das angemessene Datenschutzniveau bejahen und den Angemessenheitsbeschluss für das Vereinigte Königreich fassen. Datenexporte in das Vereinigte Königreich sind daher zu diesem Zeitpunkt auf Grundlage des Art. 45 Abs. 1 DSGVO zulässig. Doch die Kommission muss das Datenschutzniveau stetig überwachen und bei Änderungen gegebenenfalls reagieren. Spätestens nach vier Jahren ist eine erneute Evaluierung des Datenschutzniveaus im Drittland erforderlich. Angesichts des nun vorliegenden Reformvorschlags erscheint es zumindest fragwürdig, ob der Angemessenheitsbeschluss nach einer britischen Datenschutzreform bestehen bleiben kann.

II. Der Reformvorschlag

Mit dem Diskussionspapier „Data: A new direction“ („Daten: Eine neue Richtung“) vom 10. September 2021 schlägt die britische Regierung die Einführung eines eigenständigen neuen Datenschutzrechts vor, welches nicht mehr grundlegend auf der DSGVO basiert. Die Reformvorschläge sollen „einen hohen Datenschutzstandard für die Bürger gewährleisten und gleichzeitig den Unternehmen Flexibilität bei der Festlegung der effektivsten Vorgehensweise bieten.“ Dies soll unter Abbau einiger bürokratischer Anforderungen geschehen. Das Diskussionspapier stellt dabei zunächst nur eine erste Idee einer Reform dar und Stellungnahmen waren hierzu daher ausdrücklich erwünscht. Aus diesem Grund sind viele der Reformvorschläge nur vage formuliert.
Das Reformpapier gliedert sich in fünf Kapitel, die jeweils ein Reformziel darstellen und verschiedene Möglichkeiten und Mittel zur Zweckerreichung präsentieren.

1. Abbau von Barrieren für Datenverarbeitungen

Das erste Kapitel des Reformpapiers befasst sich mit dem Abbau von Barrieren für Datenverarbeitungen. Grundsätzlich steht hier die Idee im Vordergrund, die Datenverarbeitungen zu erleichtern, damit verantwortliche Unternehmen nicht aufgrund von Datenschutzvorschriften ihre Innovationsleistung bremsen. Die Anpassungen sollen insbesondere die Bereiche des berechtigten Interesses, der Künstlichen Intelligenz (KI) und automatisierten Entscheidungen, der Forschung, der Zweckänderungsvorschriften, sowie der Anonymisierung und des Teilens von Daten betreffen. So sollen unter anderem Regelbeispiele beim Tatbestand des berechtigten Interesses in das Gesetz aufgenommen werden, bei welchen die sonst erforderliche Einzelfallabwägung nicht mehr vorzunehmen ist. Auch bei Datenverarbeitung durch KI und automatisierte Entscheidungen sollen die Hürden niedriger gestaltet werden. Das Verbot automatisierter Entscheidungen, wie es in der DSGVO gilt, soll durch eine Erlaubnis ersetzt werden, wenn die Entscheidung einem legitimen oder öffentlichen Interesse dient.

Für Hochschulen und Forschungseinrichtungen sind besonders angedachte Änderungen von Vorschriften zur Datenverarbeitung zu Forschungszwecken relevant: Um Rechtsunsicherheiten vorzubeugen, soll der Forschungsbegriff legal definiert werden. Bislang findet sich lediglich eine Auslegungshilfe in Erwägungsgrund 159 wieder. Zudem soll Klarheit bezüglich der heranzuziehenden Rechtsgründe für die Verarbeitung geschaffen werden: Hochschulen sollen sich entweder auf das öffentliche Interesse stützen dürfen oder es würde ein eigener Erlaubnistatbestand zu Zwecken der Forschung eingeführt werden.

Darüber hinaus schlägt die britische Regierung vor, es betroffenen Personen zu ermöglichen, ihre Einwilligung zu einer Datenverarbeitung in umfassenderen Bereichen der Forschung zu erteilen, wenn zum Zeitpunkt der Datenverarbeitung deren Zweck nicht vollständig erkennbar ist. Dies soll möglichen Zweckänderungen vorbeugen und Projekte weniger ausbremsen. Es wird daher alternativ erwogen, dass eine Weiterverwendung von personenbezogenen Daten zu Forschungszwecken stets zulässig sein soll.

2. Entlastung von Unternehmen

Im zweiten Kapitel legt die britische Regierung ihre Pläne zur Entlastung von Unternehmen dar. Die datenschutzrechtlichen Anforderungen an die Verantwortlichen sollen sich mehr als bisher an den entsprechenden Risiken orientieren. Zwar ist auch die DSGVO risikobasiert ausgerichtet, jedoch wird die Flexibilität in den Entwurfspapieren mehr in den Fokus gerückt. Dazu sollen entsprechende Datenschutzmanagement-Programme eingeführt werden, die je nach Umständen und Inhalt der Datenverarbeitungen unterschiedliche Anforderungen an die verantwortliche Person stellen. Hierdurch müssten nicht mehr zwingend Datenschutzbeauftragte bestellt, Datenschutz-Folgenabschätzungen erstellt, Datenaufsichtsbehörden bei Verarbeitungen mit hohem Risiko konsultiert oder Verarbeitungsverzeichnisse erstellt werden. Zudem soll die Meldung von Datenschutzverstößen seltener erforderlich sein. Als Alternative eröffnet die Regierung den Vorschlag, von der Einführung von flexiblen Datenschutzmanagement-Programmen abzusehen, aber dennoch Teile der obigen Vorschläge zur Reduzierung der Pflichten der Verantwortlichen umzusetzen.

Außerdem soll auch das Auskunftsrecht der betroffenen Personen modifiziert werden: Um die Belastung der Verantwortlichen mit Auskunftsanträgen zu verringern, soll das Auskunftsrecht gebührenpflichtig werden und eine Kostenobergrenze implementiert werden. Im Ergebnis soll damit den Verarbeitern die Möglichkeit eingeräumt werden, sich entweder zu weigern, eine aufwändige Anfrage zu bearbeiten oder die entsprechende Gebühr für die Beantwortung zu erheben. Im Rahmen dieser Regelungen soll jedoch nicht das Recht des Einzelnen auf Zugang zu seinen personenbezogenen Daten ausgehebelt werden. Das Regierungspapier erkennt dabei an, dass sich die Regelungsvorschläge nachteilig auf Betroffene auswirken können, die aufgrund ihres Alters oder einer Behinderung nur schwieriger einen Anspruch auf ihre Daten erheben können, begegnet dem jedoch mit der Möglichkeit, einen entsprechenden Antrag durch einen Dritten zu stellen.

Für die konkrete Ausgestaltung der zu erhebenden Gebühr verweisen die Reformunterlagen auf eine ähnliche Regelung (die „Freedom of Information and Data Protection Regulations“ von 2004), welche Kostenobergrenzen von 600 GBP bei Anfragen an die „zentrale Regierung“ und 450 GBP für anderweitige öffentliche Einrichtungen, wie lokale Behörden, vorsah. Dabei soll allein die Kostengrenze jedoch kein Grund sein, einen Antrag gänzlich abzulehnen; vielmehr soll der Verarbeiter den Antrag so weit wie möglich innerhalb der Kostengrenze bearbeiten.

Ein Antrag soll hingegen dann abgelehnt werden können, wenn er aufgrund einer Abwägung verschiedener Faktoren, etwa des Kontexts der Anfrage, der Identität des Antragstellers oder früherer Kontakte mit diesem, als missbräuchlich erscheint. Derartige Anfragen entsprächen nicht dem Schutzzweck des Zugangs zu personenbezogenen Daten.[4]
Das Reformpapier nimmt außerdem Bezug auf die allseits bekannte Cookie-Einwilligung auf Webseiten. Momentan ist es Organisationen nicht gestattet, selbst Aktivitäten mit geringem Risiko wie Analyse-Cookies ohne Einwilligung des Nutzers zu erheben, welche in der Regel über eine Pop-up-Benachrichtigung bei Zugriff auf die entsprechende Website eingeholt wird. Die britische Regierung konstatiert dahingehend eine gewisse „Einwilligungsmüdigkeit“ der Nutzer.[5] Dem möchte die britische Regierung begegnen, indem sie entweder die Verwendung von Analyse-Cookies ohne vorherige Einwilligung gestattet (gleichzusetzen mit „technisch notwendigen Cookies“) oder es Organisationen gestattet, Informationen auf oder von einem Gerät des Nutzers für weitere, begrenzte Zwecke zu speichern, ohne dass es dafür einer Einwilligung bedürfte.

3. Datentransfer in Drittstaaten

Für britische Unternehmen soll der Datentransfer in andere Länder ebenfalls vereinfacht werden. Dies kann sich damit auch auf britische Forschungseinrichtungen, aber auch Dienstleistungen auswirken. Für die Vereinfachung sollen zunächst alle bestehenden Angemessenheitsbeschlüsse bestehen bleiben sowie mehr neue Beschlüsse hinzukommen. Außerdem soll bei der Prüfung eines Angemessenheitsbeschlusses nicht mehr die Rechtslage im Drittstaat mit der eigenen Rechtslage verglichen werden, sondern allein das praktische Risiko der Rechte der betroffenen Personen maßgeblich sein. Das Regierungspapier betont dabei, dass insbesondere die Möglichkeit

4 Schon jetzt kann der Auskunftsanspruch aus der DSGVO unter bestimmten Umständen beschränkt, bzw. eine Gebühr erhoben werden, s. hierzu Mc Grath, Wir sind hier nicht die Auskunft!, DFN-Infobrief Recht 2/2022.

5 Zu dieser Problematik s. John, Ein Tool, die Banner zu knechten, DFN-Infobrief Recht 1/2022.

der Einschränkung des Rechts auf Privatheit zum Schutz allgemeiner Interessen berücksichtigt werden muss.

4. Weitere Regelungspunkte

Neben diesen auch international bedeutungsvollen Regelungsvorschlägen betreffen die letzten zwei Kapitel vornehmlich innerbritische Angelegenheiten. So soll die Datenverarbeitung für private Unternehmen, die im Auftrag und Interesse öffentlicher Einrichtungen Datenverarbeitungen vornehmen, sich auch auf Art. 6 Abs. 1 S. 1 lit. e) DSGVO stützen dürfen, ohne hierfür eine gesonderte Rechtsgrundlage vorweisen zu müssen. In der bisherigen Fassung muss bei einer Verarbeitung im öffentlichen Interesse eine zusätzliche nationale Erlaubnisnorm vorliegen. Außerdem sollen nach dem letzten Kapitel die Kompetenzen des Datenschutzbeauftragten des Vereinigten Königreichs gestärkt werden, um eine effektivere Kontrolle des neuen Datenschutzrechts gewährleisten zu können.

5. Ausblick auf das Reformvorhaben

Das Positionspapier der britischen Regierung erwünschte sich zu den jeweiligen Vorschlägen Stellungnahmen aus dem Querschnitt der britischen Gesellschaft. Insbesondere Einzelpersonen, Start-Ups, Unternehmen, Investoren, Verbraucherorganisationen, die Forschungsgemeinschaft, Kanzleien und andere Unternehmensdienstleistende wurden explizit um Stellungnahmen gebeten. Nachdem die Frist hierfür zwischenzeitlich im November 2021 abgelaufen ist, wertet die Regierung die eingegangenen Stellungnahmen derzeit aus. Es ist offen, wann hierzu eine öffentliche Stellungnahme der Regierung zu erwarten ist.

III. Auswirkungen auf Hochschulen und Forschungseinrichtungen

1. Angemessenheitsbeschluss

Sollten die Pläne der Regierung Eingang in die Gesetzgebung finden, ist fragwürdig, ob der Angemessenheitsbeschluss der Europäischen Kommission noch bestehen bleiben kann. Das britische Diskussionspapier selbst geht davon aus, dass der Angemessenheitsbeschluss der Kommission bestehen bleiben können wird, doch das ist alles andere als sicher.
Dennoch ist festzuhalten, dass die Änderungsvorschläge das Datenschutzniveau nicht zwingend schmälern. Denn auch wenn sich Verantwortliche ggf. vermehrt auf das berechtigte Interesse durch Fallgruppen stützen können, leidet die Datensicherheit hierdurch nicht zwingend. Vielmehr könnte dies die Erfüllung eines auch in Europa zu hörenden Wunsches seitens der datenverarbeitenden Einrichtungen darstellen. Doch stellen manche Vorschläge auch kritische Änderungen für das britische Datenschutzniveau dar: Zum Beispiel ist die generelle Erlaubnis der Verarbeitung personenbezogener Daten bei der Verwendung von Analyse-Cookies als bedenklich einzustufen. Angesichts der nicht abnehmenden Brisanz der rechtlichen Auseinandersetzungen zu Cookie-Einwilligungen erscheint es fraglich, ob ein derartiges Abweichen von den Einwilligungserfordernissen vor dem Hintergrund des Angemessenheitsabkommens zwischen der EU und dem Vereinigten Königreich Bestand haben kann.

2. Europäische und britische Standardvertragsklauseln

Soweit britische Dienste von Hochschulen und Forschungseinrichtungen in Anspruch genommen werden, müsste in jedem Fall eine Prüfung der Datenschutzbestimmungen und Datenschutzerklärungen vorgenommen werden, um weiterhin die rechtmäßige Datenverarbeitung sicherzustellen. Insbesondere bei Datenexporten in das Vereinigte Königreich ist dann erneut auf die geeigneten Garantien nach Art. 46 DSGVO einzugehen, denn im Falle der Zurücknahme des Angemessenheitsbeschlusses kommt hauptsächlich die Verwendung der europäischen Standardvertragsklauseln in Betracht, um die Rechte der betroffenen Person sicherzustellen und den Export in das Vereinigte Königreich zu rechtfertigen. Alternativ ist eine ausschließliche Datenverarbeitung auf Servern im Geltungsbereich der DSGVO denkbar. Ob dies technisch möglich ist, wird vom jeweiligen Dienst abhängen.

Doch auch bei der Nutzung von Standardvertragsklauseln gibt es in naher Zukunft Änderungen. Anstelle der europäischen Standardvertragsklauseln sollen ab 21. März 2022 eigene, britische Standarddatenschutzklauseln in Form eines neuen Internationalen Übermittlungsabkommens (IDTA) und eines Addendums für internationale Datenübermittlungen zu

den europäischen Standardvertragsklauseln in Kraft treten.[6] Diese werden relevant und müssen vereinbart werden, wenn eine Einrichtung personenbezogene Daten aus dem Vereinigten Königreich ins Ausland exportieren möchte und kein britischer Angemessenheitsbeschluss für das Zielland existiert. Für Deutschland besteht momentan ein solcher Beschluss.

Zwar räumt die britische Datenschutzbehörde Übergangsfristen ein um die neuen britischen Standardvertragsklauseln in Alt- und Neuverträge zu implementieren, doch werden britische Forschungseinrichtungen bei internationalen Kooperationen darauf achten müssen, ob die Verwendung der neuen britischen Standarddatenschutzklauseln bei Datenexporten aus dem Vereinigten Königreich erforderlich ist.

3. Ausblick

Unabhängig vom Erhalt des Angemessenheitsbeschlusses oder der Verwendbarkeit von Standardvertragsklauseln kann die Datenschutzreform andere weitreichende Auswirkungen auf Forschungseinrichtungen haben. Denn sollten Datenverarbeitungen zu Forschungszwecken im Vereinigten Königreich im Vergleich zur DSGVO erleichtert werden, kann dies im Rahmen international angelegter Forschungsprojekte auch für einen britischen Forschungsstandort sprechen.

Dennoch bleibt zunächst abzuwarten, in welche Richtung sich das Reformvorhaben entwickelt. Der Titel des Diskussionspapiers weist auf eine „neue Richtung“ hin. Wohin sie allerdings gehen wird, hängt maßgeblich von den eingereichten Stellungnahmen, aber auch vom politischen Konsens des britischen Gesetzgebers ab.

In jedem Fall zeigt der Brexit durch diesen Reformvorschlag an einer weiteren Stelle seine Auswirkungen. Denn kommende Änderungen des britischen Datenschutzrechts bedeuten, dass die bisherige Vereinheitlichung des Datenschutzrechts im Vereinigten Königreich schrittweise aufgehoben wird. Auf die Hochschulen und Forschungseinrichtungen kommt damit voraussichtlich auch ein erhöhter Aufwand bei Datenexporten in das Vereinigte Königreich zu.

---

6 Die Dokumente sind auf der Seite der britischen Datenschutzbehörde zu finden, abrufbar unter https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/ (zuletzt abgerufen am 04.02.2022).

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