# DFN infobrief recht

5 / 2021
Mai 2021


## 2020: Odyssee im Beschäftigtendatenschutz

Die wichtigsten Entscheidungen zum Beschäftigtendatenschutz aus dem Jahr 2020

## TTDSG – Die Profis in spe

Zum aktuellen Stand des Gesetzgebungsverfahrens und dem Inhalt des Regierungsentwurfs des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG)

## Der Tragödie letzter Teil?

Die Auswirkungen des Brexit auf Datenübermittlungen in das Vereinigte Königreich

# 2020: Odyssee im Beschäftigtendatenschutz

Die wichtigsten Entscheidungen zum Beschäftigtendatenschutz aus dem Jahr 2020

*von Nico Gielen*

An der Schnittstelle zwischen Arbeitsrecht und Datenschutzrecht ist der Beschäftigtendatenschutz verortet. Der DFN-Verein stellt zu diesem Themenkomplex bereits eine umfassende Handlungsempfehlung zur Verfügung, die über die Grundlagen des Beschäftigtendatenschutzes informiert.[1] Diese theoretischen Grundlagen stellen einerseits eine hilfreiche Orientierung dar. Andererseits ist die konkrete Auslegung der teilweise unbestimmten Gesetze von den Gerichten abhängig. Daher werden im Folgenden die Entscheidungen aus dem Jahr 2020 dargestellt, die für den Beschäftigtendatenschutz wegweisend sind und daher eine große Praxisrelevanz – auch für Hochschulen und Forschungseinrichtungen – aufweisen.

## I. Einwilligung im Beschäftigungskontext

Nach dem im Datenschutzrecht geltenden Grundsatz des Verbotes mit Erlaubnisvorbehalt ist eine Datenverarbeitung verboten, wenn sie nicht durch einen Erlaubnistatbestand legitimiert ist. Die Erlaubnistatbestände sind in Art. 6 Abs. 1 Datenschutzgrund-Verordnung (DSGVO) aufgeführt. Demnach ist eine Datenverarbeitung insbesondere rechtmäßig, wenn die betroffene Person eine wirksame Einwilligung abgegeben hat (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO).

Über das Vorliegen einer wirksamen Einwilligung im Beschäftigungskontext musste das Landesarbeitsgericht (LAG) Köln entscheiden (Urt. v. 7.2.2020, Az. 4 Sa 329/19). In diesem Fall überließ der Arbeitgeber dem Beschäftigten einen Laptop und beide vereinbarten Folgendes: „Die vom Arbeitgeber zur Verfügung gestellten Arbeitsmittel dürfen nicht für private Zwecke genutzt werden. […] Der Arbeitnehmer erklärt auch sein Einverständnis damit, dass der Arbeitgeber die auf den Arbeitsmitteln befindlichen Daten aus Zwecke [sic] der Zuordnung zu geschäftlichen oder privaten Vorgängen überprüft und auswertet." Es liegt nahe, darin eine Einwilligung des Beschäftigten zu erblicken. Allerdings muss im Beschäftigungskontext zur Beurteilung, ob eine Einwilligung auch freiwillig erteilt wurde (Art. 7 Abs. 4 DSGVO), die Abhängigkeit des Beschäftigten berücksichtigt werden (§ 26 Abs. 2 S. 1 BDSG). Wenn man dies berücksichtige, so das LAG Köln, sei die Vereinbarung zwischen dem Arbeitgeber und dem Beschäftigten zu unpräzise und zu weit gefasst. Der Beschäftigte könne durch diese nicht erkennen, welche Daten der Arbeitgeber überprüfen wird. Insbesondere habe er nicht absehen können, ob und in welchem Umfang private Daten überprüft werden. Damit konnte das LAG Köln keine wirksame Einwilligung feststellen.

## II. Erforderlichkeit der Datenverarbeitung (§ 26 Abs. 1 BDSG)

Eine Ergänzung der in Art. 6 Abs. 1 DSGVO statuierten Erlaubnistatbestände erfolgt durch Art. 88 Abs. 1 DSGVO, der die Mitgliedstaaten dazu berechtigt, im Beschäftigungskontext durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Regelungen vorzusehen (sog. Öffnungsklausel). Als Ausgestaltung dieser Öffnungsklausel wurde auf Bundesebene § 26 Bundesdatenschutzgesetz (BDSG) erlassen. Zusätzlich zu den in Art. 6 Abs. 1 DSGVO genannten Erlaubnistatbeständen ist eine Verarbeitung von Beschäftigtendaten danach insbesondere zulässig, wenn sie für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist (§ 26 Abs. 1 S. 1 BDSG). Der Begriff der

1 Diese Handlungsempfehlung findet sich in der DFN-Wissensbasis.

Erforderlichkeit entscheidet damit oftmals über die Zulässigkeit der Verarbeitung von Beschäftigtendaten und ist daher zentral in der Rechtsprechung der Arbeitsgerichtsbarkeit.

Dies sah man auch beim Arbeitsgericht (ArbG) Wesel, welches zu entscheiden hatte, ob ein Arbeitgeber mithilfe seiner Kameraüberwachung die aufgrund der Pandemie empfohlenen Sicherheitsabstände zwischen den Beschäftigten überprüfen darf (Beschl. v. 24.4.2020, Az. 2 BVGa 4/20). In dem vorliegenden Fall wurden die Aufnahmen ins Ausland versendet, um dort anonymisiert zu werden. Das ArbG Wesel entschied, dass die Videoüberwachung nicht erforderlich sei. Insbesondere könne man – wenn die Beschäftigtendaten anonymisiert seien – keine individuellen Beschäftigten auf ihr Fehlverhalten ansprechen, sondern nur organisatorische Veränderungen vornehmen. Dies könne man aber auch ohne eine Videoüberwachung.

Vor dem LAG Nürnberg ging ein Beschäftigter gegen seine Kündigung vor, die der Arbeitgeber auf den Diebstahl von zwei Jägermeisterfläschchen aus dem Getränkelager stützte (Urt. v. 8.12.2020, Az. 7 Sa 226/20). Als Beweis legte der Arbeitgeber eine Videoaufzeichnung vor. Das LAG Nürnberg wies darauf hin, dass eine Datenverarbeitung zur Aufdeckung einer Straftat voraussetze, dass tatsächliche Anhaltspunkte einen Tatverdacht begründen und die Verarbeitung zur Aufdeckung erforderlich ist (§ 26 Abs. 1 S. 2 BDSG). Einen Verdacht bejahte das LAG, denn dieser ergebe sich daraus, dass im Getränkelager zunehmend ein Schwund verzeichnet wurde. Allerdings sah das LAG die verdeckte Videoüberwachung nicht als erforderlich an, weil es der Überzeugung war, dass mildere Mittel möglich gewesen wären. Der Arbeitgeber habe zumindest nicht überzeugend dargelegt, dass man den Täterkreis nicht auf andere Weise hätte eingrenzen können. Daher bestand keine Erforderlichkeit für die Datenverarbeitung.

Mit einer Verdachtssituation hatte sich auch das LAG Berlin-Brandenburg zu beschäftigen (Urt. v. 11.9.2020, Az. 9 Sa 584/20). Bei einem im Home-Office arbeitenden Beschäftigten stellte der Arbeitgeber einen Rückgang der Arbeitsleistung fest und engagierte daher eine Detektei, welche den Beschäftigten beschatten sollte. Durch diese Beschattung stellte sich heraus, dass der Beschäftigte unberechtigte Spesenabrechnungen eingereicht hatte. Dem schloss sich eine fristlose Kündigung und ein Kündigungsschutzprozess an, in dem sich der Beschäftigte auf das Datenschutzrecht berief. Das LAG prüfte daraufhin, ob die Datenerhebung des Arbeitgebers durch die Detektei erforderlich gewesen sei. Im Falle einer verdeckten Überwachung zur Aufklärung einer schwerwiegenden – wenn auch nicht strafbaren – Pflichtverletzung müsse ebenfalls „ein auf konkrete Tatsachen gegründeter Verdacht für das Vorliegen einer solchen Pflichtverletzung bestehen“. Entsprechende Anhaltspunkte lagen laut dem LAG aber nicht vor. Zwar sei die Arbeitsleistung des Arbeitnehmers zurückgegangen, aber das begründe noch keinen Verdacht einer schwerwiegenden Pflichtverletzung. Die Kündigung war daher unwirksam.

Des Weiteren entschied das LAG Berlin-Brandenburg, dass die Einführung eines Zeiterfassungssystems, welches von den Beschäftigten Fingerabdrücke verlangt, nicht erforderlich sei (Urt. v. 4.6.2020, Az. 10 Sa 2130/19). Ein Fingerabdruck sei ein biometrisches Datum (Art. 4 Nr. 14 DSGVO) und daher gemäß Art. 9 DSGVO besonders streng zu bewerten. Grundsätzlich sei eine Verarbeitung solcher Daten untersagt und nur ausnahmsweise zulässig. Vor diesem Hintergrund wies das Gericht daraufhin, dass durchaus Zeiterfassungssysteme existieren würden, die auch ohne eine Verarbeitung sensibler Daten auskommen. Zwar sei das Zeiterfassungssystem mittels Fingerabdrücken eventuell effektiver, da es besser gegen Manipulationen schütze. Eine solche Manipulation stelle aber eine schwerwiegende Pflichtverletzung dar, sodass tatsächliche Anhaltspunkte einen konkreten Verdacht begründen müssen, damit eine Datenverarbeitung zur Aufdeckung erforderlich sein könnte. Solche Anhaltspunkte bestanden im vorliegenden Fall jedoch nicht.[2]

## III. Anspruch auf Auskunft (Art. 15 DSGVO)

Nach Art. 15 DSGVO hat die betroffene Person das Recht, von dem Verantwortlichen Auskunft über ihre vom Verantwortlichen verarbeiteten personenbezogenen Daten zu verlangen. Dieser Auskunftsanspruch wird immer mehr auch von Beschäftigten gegen den Arbeitgeber geltend gemacht.

Das ArbG Münster entschied, dass ein Arbeitgeber dieser Pflicht nicht nachkommt, wenn er die Auskunft erst nach drei Monaten erteilt (Urt. v. 11.8.2020, Az. 1 Ca 247 c/20). Aus Art. 12 Abs. 3 S. 1 DSGVO ergebe sich, dass die Auskunft grundsätzlich binnen eines Monats erfolgen muss.

2 Siehe zu der Entscheidung in der Vorinstanz bereits John, DFN-Infobrief Recht 2/2020, S. 2 ff.

Das ArbG Bonn nahm darüber hinaus Stellung zur Reichweite des Auskunftsanspruchs (Urt. v. 16.7.2020, Az. 3 Ca 2026/19). Es differenzierte dabei zwischen einer „allgemeinen Auskunftspflicht“ und „weitergehenden Auskunftsansprüchen“, wofür das Auskunftsbegehren zunächst präzisiert werden müsse. Dabei berief es sich auf Erwägungsgrund 63 S. 7 der DSGVO: „Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.“ In dem vorliegenden Fall sei beim Arbeitgeber eine Vielzahl personenbezogener Daten über den Beschäftigten vorhanden gewesen. Daher sei er nicht verpflichtet gewesen, alle Informationen zu übermitteln, sondern nur solche allgemeiner Natur. Weitere Informationen hätte der Beschäftigte präzise anfragen müssen. Da diese Präzisierung aber nicht erfolgte, sei der Auskunftsanspruch durch die allgemeine Auskunft des Arbeitgebers bereits erfüllt worden.

## IV. Schadensersatzanspruch (Art. 82 Abs. 1 DSGVO)

Nach Art. 82 Abs. 1 DSGVO hat jede Person Anspruch auf Schadenersatz gegen den Verantwortlichen, wenn ihr wegen eines Verstoßes gegen die DSGVO ein materieller oder immaterieller Schaden entstanden ist.

In einem vom LAG Köln entschiedenen Fall unterhielt der Arbeitgeber eine Webseite mit den jeweiligen Profilen seiner Beschäftigten (Urt. v. 14.9.2020, Az. 2 Sa 358/20). Von einer Beschäftigten trennte sich der Arbeitgeber und löschte daraufhin ihre Profilseite. Aufgrund einer Umgestaltung der Webseite war eine ältere Seite aber noch abrufbar. Ohne den Arbeitgeber darauf hinzuweisen, zog die ehemalige Beschäftigte vor Gericht und forderte Schadensersatz. Das LAG Köln bejahte einen Verstoß gegen die DSGVO, denn die Anzeige des Profils sei für die Durchführung des Beschäftigungsverhältnisses nicht mehr erforderlich gewesen. Es sei unerheblich, dass der Schadensposten marginal sei, denn Art. 82 Abs. 1 DSGVO kenne keine Bagatellgrenze. Allerdings schätzte das Gericht die Beeinträchtigung für die Beschäftigte als gering ein. Auch stufte es die Anwaltskosten nicht für ersatzfähig ein, da die Beschäftigte den Arbeitgeber hätte informieren können, bevor sie gerichtliche Schritte einleitete. Im Ergebnis sprach das Gericht einen Schadensersatz in Höhe von 300 Euro zu.

Das ArbG Dresden entschied über einen Schadensersatzanspruch, den ein ausländischer Beschäftigter gegen seine ehemalige Arbeitgeberin geltend machte (Urt. v. 28.8.2020, Az. 13 Ca 1046/20). Die Arbeitgeberin kündigte ihm, als dieser krankheitsbedingt ausfiel und informierte daraufhin die Ausländerbehörde sowie die Arbeitsagentur ausführlich über die Fehlstunden. Diese Krankheitszeiten seien nach dem ArbG Dresden jedoch Gesundheitsdaten im Sinne von Art. 9 DSGVO. Außerdem sei die Datenübermittlung an die Behörden weder durch eine Einwilligung des Beschäftigten gedeckt noch erforderlich gewesen. Hinsichtlich der Schadenshöhe orientierte sich das Gericht an Art. 83 Abs. 2 S. 2 DSGVO, wonach insbesondere die Schwere des Verstoßes, die Vorsätzlichkeit und die Sensibilität der Daten für einen hohen Schadensersatz gesprochen hätten. Insgesamt sprach das Gericht einen Schadensersatz in Höhe von 1700 Euro zu.

In einem Fall, welchen das LG (Landgericht) Darmstadt entschied, bewarb sich eine Person bei einer Bank über eine Online-Karriereplattform (Urt. v. 26.5.2020, Az. 13 O 244/19). Die Antwort der Bank ging allerdings nicht nur an sie heraus, sondern aus Unachtsamkeit auch an eine dritte Person, die zufälligerweise ein Kollege des Bewerbers war. Der Bewerber wurde vom Kollegen auf die Weiterleitung hingewiesen. Von der Bank wurde er über diesen Vorgang hingegen nicht informiert. Das LG Darmstadt stellte einen Verstoß gegen Art. 6 DSGVO fest, weil keine Rechtsgrundlage für die Übermittlung der Bewerbungsunterlagen an die dritte Person bestanden habe. Außerdem habe die Bank gegen Art. 34 DSGVO verstoßen, weil sie den Bewerber nicht über die Datenschutzverletzung informiert hat. Die Datenschutzverletzungen seien auch schwerwiegend, weil sie den Kläger beruflich stark benachteiligen können. Das Gericht sprach einen Schadensersatz von rund 1000 Euro zu.[3]

Schließlich hatte das ArbG Düsseldorf noch über die Verletzung eines Auskunftsanspruchs zu entscheiden (Urt. v. 5.3.2020, Az. 9 Ca 6557/18). Bei der Bemessung des Schadensersatzes betonte es, dass dieser „wirksam, verhältnismäßig und abschreckend“ sein müsse. Hierbei sei relevant, dass der Arbeitgeber einen hohen Umsatz aufwies: „Da der Schadensersatz eine angemessene Wirkung erzielen soll, hängt dessen Höhe nicht nur vom eingetretenen immateriellen Schaden, sondern auch von dem nach Art. 4 Nr. 7 DS-GVO Verantwortlichen und dessen

3 Siehe zu dieser Entscheidung ausführlich Uphues, DFN-Infobrief Recht 4/2021, S. 9 ff.

Finanzkraft ab. Mit anderen Worten: Die Verletzung der Auskunftspflicht aus Art. 15 DS-GVO durch einen finanzschwächeren Verantwortlichen würde zu geringerem Schadensersatz führen." Auch mit Hinweis auf die monatelange Verletzung des Auskunftsanspruchs sprach das Gericht einen Schadensersatz in Höhe von 5000 Euro zu, wobei das Gericht für einen Monat Verspätung 500 Euro als Richtwert ansetzte.[4]

## V. Fazit

An der aktuellen Rechtsprechung wird deutlich, dass die DSGVO neue Akzente im Beschäftigtendatenschutz setzt. Insbesondere umfangreiche Auskunftsansprüche und mitunter hohe Schadensersatzansprüche fallen dabei auf. Es ist mit Spannung zu verfolgen, inwiefern sich in den nächsten Jahren feste Maßstäbe in der Arbeitsgerichtsbarkeit entwickeln werden, um die Interessen zwischen Arbeitgeber und Beschäftigten in Ausgleich zu bringen.

---

4 Siehe zu dieser Entscheidung ausführlich John, DFN-Infobrief Recht 10/2020, S. 9 ff.

# TTDSG – Die Profis in spe

Zum aktuellen Stand des Gesetzgebungsverfahrens und dem Inhalt des Regierungsentwurfs des Telekommunikations-Telemedien-Datenschutzgesetzes (TTDSG)

*von Nicolas John*

Die Landschaft des Datenschutz- und Telekommunikationsrechts unterliegt, auch bedingt durch den technischen Fortschritt, einem stetigen Wandel. Nach dem Inkrafttreten der Datenschutz-Grundverordnung 2018 (DSGVO) ist der Erlass der lang erwarteten ePrivacy-Verordnung (ePrivacyVO) auf europäischer Ebene ins Stocken geraten. Wann es zu einer Einigung über diese kommen wird, ist derzeit ungewiss. In der Zwischenzeit bleibt aber auch der nationale Gesetzgeber nicht untätig. Zumindest auf nationaler Ebene soll der unübersichtliche Datenschutzdschungel etwas gelichtet werden. Ein Fall für TTDSG!

## I. Entwicklung der Datenschutzgesetze

### 1. Datenschutzrichtlinie und ePrivacy-Richtlinie

Vor der Wirksamkeit der DSGVO bestimmten in Europa vor allem die Datenschutzrichtlinie[1] von 1995 und die sog. ePrivacy-Richtlinie[2] von 2002 das Telekommunikations- und Datenschutzrecht. Als europäische Richtlinien erlangten diese jedoch keine unmittelbare Rechtswirkung in den Mitgliedsstaaten, sondern mussten in nationales Recht umgesetzt werden. In Deutschland führte die Umsetzungspflicht sowohl zur Novellierung des Bundesdatenschutzgesetzes (BDSG) als auch des Telekommunikationsgesetzes (TKG). Parallel zu den Umsetzungen der Richtlinien wurde auch das nationale Datenschutzrecht 2007 weiter überarbeitet und so mit dem Erlass des Telemediengesetzes (TMG) drei verschiedene bis dahin geltende Regelwerke[3] zusammengefasst, welche ebenfalls Bereiche des Telekommunikations- und Datenschutzrechts für Anbieter von Telekommunikationsdiensten (TK-Dienste) regelten.

1 Richtlinie 95/46/EG.
2 Richtlinie 2002/58/EG.
3 Das Teledienstgesetz (TDG), das Teledienstdatenschutzgesetz (TDDSG) und weitestgehend der Mediendienste-Staatsvertrag (MDStV).

2009 nahm der europäische Gesetzgeber mit der sog. Cookie-Richtlinie[4] Änderungen an der ePrivacy-Richtlinie vor, welche insbesondere die Nutzung von Cookies auf Webseiten betraf. Vor allem eine höhere Transparenz und Sicherheit für die Verbraucher stand im Fokus der Anpassungen. Der deutsche Gesetzgeber sah die erforderliche Umsetzung mit den Vorschriften des schon existierenden TMG als erfüllt an. Datenschützer kritisieren diese Ansicht als schwache Umsetzung, ihrer Meinung nach stelle die Cookie-Richtlinie strengere Anforderungen an die Einwilligung zur Datenverarbeitung bei Cookies auf Webseiten als es das deutsche TMG vorschreibt.

Trotz der einheitlichen Vorgaben der Richtlinien entwickelten sich in Europa sehr unterschiedliche Prioritäten des Datenschutzrechts in den einzelnen Mitgliedsstaaten. Die Wahrnehmung der Umsetzungsspielräume der Richtlinien sorgte für stark voneinander abweichende Datenschutzniveaus in den Mitgliedsstaaten.

### 2. Einführung der DSGVO

Diese nationalen Unterschiede sollten mit der Einführung der DSGVO nach langen Verhandlungen harmonisiert werden. Als

4 Richtlinie 2009/136/EG.

europäische Verordnung ist diese seit dem 25. Mai 2018 unmittelbar in allen Mitgliedsstaaten anwendbar und ersetzt die alte Datenschutzrichtlinie. Dennoch eröffnet die DSGVO mit verschiedenen Öffnungsklauseln den Mitgliedsstaaten weiterhin an vielen Stellen die Möglichkeit, von einzelnen Vorschriften im nationalen Recht abzuweichen und spezifische Aspekte (z. B. den Beschäftigtendatenschutz) selbst zu regeln. Daher wurde in Deutschland vor allem das BDSG mit Blick auf die Öffnungsklauseln neu gefasst, aber auch bereichsspezifische Regelungen und die Landesdatenschutzgesetze (LSDG) wurden an die DSGVO angepasst.

## 3. ePrivacy-Verordnung

In Erwägungsgrund 173 der DSGVO hat sich der europäische Gesetzgeber darüber hinaus verpflichtet, auch die ePrivacy-Richtlinie zu überprüfen, um einen einheitlichen Datenschutz zu gewährleisten. Hierfür hatte die europäische Kommission schon 2017 einen Vorschlag der ePrivacyVO verabschiedet, doch der EU-Ministerrat konnte sich lange Zeit auf keine gemeinsame Position festlegen.[5] Erst im Februar 2021 konnten sich die Mitgliedsstaaten auf ein Mandat einigen, womit nun Verhandlungen mit dem europäischen Parlament und der Kommission im Rahmen der Trilog-Gespräche über den endgültigen Wortlaut der Verordnung aufgenommen werden können. Allerdings steht weiter in den Sternen wann die Verordnung tatsächlich in Kraft treten wird.

## 4. TTDSG

Aufgrund dieser fehlenden Vereinheitlichung der Datenschutzvorschriften auf europäischer Ebene herrscht vor allem im Bereich der ePrivacy oftmals Rechtsunsicherheit in der Frage, wann Dienstanbieter elektronischer Kommunikationsdienste bestimmten Regeln unterliegen und welche Regeln in der Anwendung Vorrang haben. Entscheidungen des Europäischen Gerichtshofs (EuGH) wie „Gmail“[6] oder „Skype-Out“[7], welche sich um die Anwendbarkeit des TKG drehten, zeigen offenkundig diese Unsicherheiten. Insbesondere das TMG ist zu weiten Teilen aufgrund des Vorrangs der DSGVO nicht mehr anwendbar. Dennoch haben weiterhin Vorgaben der Cookie-Richtlinie im TMG Niederschlag gefunden und sind weiterhin anwendbar. Auch das TKG ist aufgrund verschiedener Öffnungsklauseln und anderer geregelten Teilbereiche, wie beispielsweise dem Fernmeldegeheimnis, trotz Geltung der DSGVO weiterhin anwendbar.

Aufgrund dieser Unsicherheiten in der Anwendung und Abgrenzung beabsichtigt der deutsche Gesetzgeber nun die Zusammenführung des TMG und TKG in das neue TTDSG. Ziel ist es, mehr Rechtsklarheit zu schaffen, erforderliche Anpassungen an die DSGVO vorzunehmen und die Schaffung einer nationalen Übergangsregelung bis zum Inkrafttreten der ePrivacyVO.

Nachdem Ende Juli 2020 ein Referentenentwurf geleakt wurde, hat die Bundesregierung den offiziellen Entwurf Mitte Januar 2021 veröffentlicht. Nach der Anhörung der Verbände durch das Bundesministerium für Wirtschaft und Energie beschloss und veröffentlichte das Bundeskabinett am 10. Februar 2021 den Regierungsentwurf.[8] Der Bundesrat gab im März 2021 zu diesem Entwurf eine Stellungnahme[9] ab. Ende März beriet der Bundestag in erster Lesung den Entwurf und leitete die Vorlage in den Ausschuss für Wirtschaft und Energie weiter.

## 5. EKEK-Richtlinie und TKG-Novelle

Parallel zu den oben genannten Richtlinien hat der europäische Gesetzgeber mit dem Europäischen Kodex für die elektronische Kommunikation[10] (EKEK-Richtlinie) weitere Anpassungen hinsichtlich der Regelungen von elektronischen Kommunikationsnetzen und -diensten vorgenommen. In Deutschland wird die Richtlinie mit einer erneuten Novelle des TKG umgesetzt, welche derzeit noch im Gesetzgebungsprozess steckt. Diese wird mit dem Telekommunikationsmodernisierungsgesetz (TKMoG) stattfinden. Momentan befindet sich das TKMoG ebenfalls noch in der Gesetzgebungsphase,

5 Vertiefend hierzu: Uphues, Das Warten hat kein Ende, DFN-Infobrief Recht 3/2020.

6 EuGH, Urteil v. 13.06. 2019 – C-193/18; vertiefend hierzu s. Mörike, No Signal, DFN-Infobrief Recht 07/2019.

7 EuGH, Urteil v. 05.06.2019 – C-142/18.

8 BT Drs. 19/27441.

9 BR Drs. 163/21(B).

10 Richtlinie (EU) 2018/1972.

ein Referentenentwurf[11] wurde Ende 2020 beschlossen. Das kommende überarbeitete TKG (TKG-E) wird den Rahmen von Telekommunikationsdiensten regeln, wobei der Datenschutz und das Fernmeldegeheimnis dagegen gebündelt im TTDSG geregelt werden soll. Auswirkungen der EKEK-Richtlinie auf das TTDSG ergeben sich vor allem im Anwendungsbereich des TTDSG.

## II. Regelungsinhalte des TTDSG

Ziel des TTDSG ist die Behebung der bestehenden Rechtsunsicherheit im Datenschutzrecht durch das Nebeneinander der DSGVO, TKG und TMG. Hierdurch soll eine höhere Transparenz für Anwender und Betroffene im Datenschutzrecht geschaffen werden. Erreicht wird dies unter anderem durch die Überführung der Bestimmungen zum Datenschutz- und Fernmelderecht aus den §§ 88 ff. TKG und den Datenschutzbestimmungen für Telemedien aus §§ 11 ff. TMG.

Der Gesetzesentwurf ist in vier Teile aufgeteilt: Den Teil der „Allgemeinen Vorschriften“, den Teil zum „Datenschutz und Schutz der Privatsphäre in der Telekommunikation“, den „Telemedienschutz, Endeinrichtung“ und den Teil „Straf- und Bußgeldvorschriften und Aufsicht“.

### 1. Anwendungsbereich

Der Anwendungsbereich des TTDSG soll neben der DSGVO nun auch sog. Over-the-top-Dienste (OTT) wie Messenger-Dienste explizit erfassen. OTT-Dienste sind Dienste, welche Kommunikationsinhalte von Nutzenden über das Internet übermitteln, ohne dass eine Kontrolle durch den Internetdienstleister möglich ist oder dieser für die Verbreitung eingebunden sein muss. Die Eröffnung des Anwendungsbereichs geht auf die Umsetzung der EKEK-Richtlinie zurück, welche OTT-Dienste wie klassische TK-Dienste behandelt. Gemäß § 2 Abs. 1 TTDSG-E i.V.m. § 3 Nr. 24, 61 TKG E fallen als „interpersonelle Telekommunikationsdienste“ in den Anwendungsbereich des TTDSG auch webgestützte E-Mail-Dienste, Internettelefonie oder Kommunikationseinrichtungen in Online-Spieleplattformen.

11 Abrufbar unter https://www.bmwi.de/Redaktion/DE/Downloads/Gesetz/telekommunikationsmodernisierungsgesetz-referentenentwurf-20201612.pdf?__blob=publicationFile&v=8 (zuletzt abgerufen am 14.04.2021).

### 2. Einwilligung bei Verwendung von Cookies

Inhaltliche Besonderheiten stellen insbesondere die Regelungen zum Einsatz von Cookies und vergleichbaren Technologien dar. § 24 TTDSG-E orientiert sich dabei eng am Wortlaut der ePrivacy-Richtlinie und umfasst nach Abs. 1 technologieneutral jegliche „Speicherung [oder Zugriff] von Informationen in der Endeinrichtung“. Derzeit sind damit vor allem Cookies bei der Nutzung von Webseiten erfasst, aber auch schon in der Wirtschaft angedachte Techniken des „Browser Fingerprinting“ werden von der Regelung erfasst.

Als Cookies werden kleine Textdateien bezeichnet, welche auf dem Computer des Nutzenden eines Online-Dienstes gespeichert werden. Durch sie können Webseitenbetreibende erkennen, wer ihre Seite gerade besucht und dadurch Präferenzen des Nutzenden wie beispielsweise die Login-Daten speichern, damit diese nicht bei jedem Besuch der Webseite erneut vorgenommen werden müssen. Auch der Inhalt eines Warenkorbs bei Online-Shops wird mit Hilfe von Cookies beim Nutzen des Shops gespeichert. Es ist durch Cookies allerdings auch möglich, dass Webseitenbetreibende anhand der gespeicherten Cookies erkennen können, welche Webseiten der Nutzende besucht hat und dadurch Interessen und Vorlieben des Nutzenden durch das umfangreiche Tracking erfahren. Diese Informationen werden vor allem in der Werbebranche für personalisierte Werbung genutzt. Zunehmend werden auch Trackingverfahren (z.B. das Browser Fingerprinting) entwickelt, die ohne eine Nutzung von Cookies auskommen.

§ 24 Abs. 1 TTDSG-E verlangt für die Speicherung oder den Zugriff auf Informationen wie Cookies stets eine Einwilligung des Nutzenden. Ausnahmen von diesem Einwilligungserfordernis gelten nur dann, wenn mit Hilfe dieser Daten eine Nachricht übertragen werden soll (§ 24 Abs. 2 Nr. 1 TTDSG-E) oder die Speicherung bzw. der Zugriff auf die Daten für die Nutzung des „vom Nutzer ausdrücklich gewünschten Telemediendienstes“ „unbedingt erforderlich“ ist (§ 24 Abs. 2 Nr. 2 TTDSG-E).

Bemerkenswert ist bei dieser Regelung, dass der Anwendungsbereich nicht, wie im Rahmen der DSGVO, von einem Personenbezug abhängig gemacht wird. Dadurch soll der Nutzende unabhängig vom Vorliegen von personenbezogenen Daten bei jedem Eingriff geschützt werden. Außerdem stellt die Bundesregierung in den Erwägungen zu § 24 TTDSG-E klar, dass neben den klassischen Endgeräten auch sämtlichen mit dem Inter-

net verbundene Geräte des Internet-of-things (IoT) unter den Anwendungsbereich des Einwilligungserfordernisses fallen sollen.

Die Regelung macht die Nutzung von Tools zur Webseiten-Optimierung wie Analytics oder Reichweitenmessung weiterhin von der Einwilligung der Nutzenden abhängig. In der Praxis würde dies weiterhin für die bekannten unübersichtlichen Cookie-Banner sorgen, welche Nutzende oftmals gezielt verwirren sollen, um eine Einwilligung zu erreichen. Der Bundesrat hat in seiner Stellungnahme zum Regierungsentwurf daher vorgeschlagen, diese komplexen Banner zu verbieten. Er sieht vielmehr „eine einfache Gestaltung beispielsweise mithilfe von nur zwei Buttons (‚Einwilligen', ‚Ablehnen') [als] zielführend" an.[12] Doch ob eine solche Regelung im Hinblick auf die Vorgaben der ePrivacy-Richtlinie überhaupt zulässig ist, ist unklar. Eine Alternative hierzu könnte eine ebenfalls vom Bundesrat vorgeschlagene generelle Einwilligung (oder Ablehnung) von Cookies über die Browser-Einstellungen darstellen.

## 3. Technische und organisatorische Vorkehrungen

§ 19 Abs. 2 TTDSG-E fällt mit seiner Regelung auf, dass Anbietende von Telemedien durch technische und organisatorische Vorkehrungen die Nutzung des Dienstes anonym oder unter Pseudonym ermöglichen sollen, soweit dies technisch möglich und zumutbar ist. Die Vorschrift basiert auf § 13 Abs. 5 und Abs. 6 TMG und wird in der Praxis kaum eine Rolle spielen, aufgrund von beispielweise Gerätekennungen wird eine Anonymisierung meist schon technisch unmöglich sein. Darüber hinaus läuft die anonyme oder pseudonymisiert Nutzung bei sozialen Netzwerken oder Messengerdiensten dem grundlegenden Zweck des Dienstes entgegen, denn das Geschäftsmodell solcher Plattformen zielt gerade auf die Identifizierbarkeit der Nutzenden ab.

Auch die Anzeigepflicht der Weitervermittlung auf eine andere Webseite gem. § 19 Abs. 3 TTDSG wird aufgrund der in der Praxis immer weiter verbreiteten Einbindung (Framing) von anderen Webseiten in die eigene Webpräsenz leerlaufen, da die Einbindung nicht als klassische Weiterleitung zu qualifizieren ist.

12 BR Drs. 163/21(B), S. 5.

## 4. Fernmeldegeheimnis

Durch die Ausweitung des Anwendungsbereiches des TTDSG-E auf OTT-Dienste wird das Fernmeldegeheimnis in dem Entwurf gem. § 3 TTDSG-E nicht mehr nur für klassische TK-Dienste wie Telefon und SMS gelten, sondern nun auch für Messenger, Internettelefonie oder webbasierte E-Mail-Dienste, § 2 Abs. 1 TTDSG-E i.V.m. § 3 Nr. 24, 61 TKG-E. Als Konsequenz ist es Anbietenden von solchen TK-Diensten nicht gestattet, sich über das technisch erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Kommunikation zu verschaffen, § 3 Abs. 3 S. 1 TTDSG-E. Eine Durchleuchtung von E-Mails zu Werbezwecken ist für Mailanbieter wie Google damit nicht mehr ohne weiteres, wie beispielsweise einer Zustimmung des Nutzenden, möglich.

Im Übrigen soll das Fernmeldegeheimnis nicht der Wahrnehmung von Rechten der Erben eines Nutzenden entgegenstehen, § 4 TTDSG-E.[13]

## 5. Neue Aufsichtszuständigkeiten

Der Regierungsentwurf des TTDSG überträgt dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) einheitlich den Vollzug des 1. Und 2. Teils des TTDSG, soweit personenbezogener Daten verarbeitet werden oder Anbietende von Telemedien § 24 TTDSG-E beachten müssen. Ursprünglich war der oder die BfDI nur für den Vollzug des TKG zuständig, für den Vollzug des TMG die Landesdatenschutzaufsichtsbehörden ermächtigt. Durch diese Anpassung werden die Verarbeitungen von personenbezogenen Daten und der Zugriff auf Endeinrichtungen von einer Aufsichtsbehörde einheitlich kontrolliert. Soweit in diesen Bereichen die Zuständigkeit des oder der BfDI nicht gegeben ist, bleibt die bisherige Aufsicht der Bundesnetzagentur (BNetzA) bestehen. Hinsichtlich des 3. Teils des TTDSG-E fehlen ausdrückliche Zuteilungen der Aufsicht, insoweit dürfte die Aufsicht weiterhin bei den Landesdatenschutzbehörden liegen.

13 Zu der Ausgangsproblematik s. Strobel, Digitaler Nachlass – letzter Akt, DFN-Infobrief Recht 9/2018.

## III. Fazit und Konsequenzen für Hochschulen

Die Einführung des TTDSG mag auf den ersten Blick einen positiven Eindruck machen, doch setzen zum Beispiel die Regelungen zur Verwendung von Cookies und ähnlichen Technologien lediglich die Situation fest, welche seit 2009 aufgrund der ePrivacy-Richtlinie und durch die Urteile des EuGH und BGH längst in der Praxis geformt worden ist. Digitalverbände kritisieren daher berechtigterweise, dass das Gesetz nicht die aktuellen Entwicklungen berücksichtige, sondern auf dem Stand der ePrivacy-Richtlinie von 2009 beruhe. Praktische Änderungen sind auf Grundlage des Regierungsentwurfs in der Verwendung von Cookies daher momentan nicht zu erwarten. Abzuwarten bleibt, welche Änderungen in der kommenden Zeit vorgenommen werden, bevor die endgültige Fassung des TTDSG in Kraft tritt. Gerade Forderungen wie die des Bundesrates zu einfachen Cookie-Bannern werden die Diskussionen weiterhin anfachen. Zu viel sollte aufgrund der engen Vorgaben der ePrivacy-Richtlinie allerdings nicht erwartet werden. Globale Browser-Einstellungen, wie ebenfalls vom Bundesrat vorgeschlagen, können eine Lösung darstellen, denn auch schon der europäischen Gesetzgeber thematisiert diese Möglichkeit in Erwägungsgrund 66 der Cookie-Richtlinie. Mit dem vorgelegten Regierungsentwurf ist jedoch nicht mit einer umfassenden Lösung für den Einsatz von Cookies zu rechnen.

Dagegen stellt die Erweiterung des Anwendungsbereiches des TTDSG auf OTT-Dienste-Anbietende eine Klarstellung in der Praxis dar. Die noch 2019 von der Rechtsprechung des EuGH behandelte Problematik um die Einordnung von Skype-Out oder Gmail als Telekommunikationsdienstleister erledigt sich damit. Dadurch sind OTT-Dienste nun wie klassische TK-Dienste an das Fernmeldegeheimnis gebunden.

Auch auf Hochschulen und Forschungseinrichtungen wird das neue TTDSG Auswirkungen haben. Schon beim Betreiben einer öffentlichen Website sind die ggf. neuen Vorschriften zu Cookies umzusetzen. Auch im Falle eines öffentlichen Angebots eines OTT-Dienstes wie einem Messenger oder webbasierte E-Mail-Dienst können Hochschulen an die Vorschriften des TTDSG gebunden sein. Inwieweit die Vorschriften dabei jeweils im Detail anzuwenden sind, muss nach Inkrafttreten des Gesetzes geprüft werden. Wie das TTDSG in seiner finalen Form aussehen wird, bleibt abzuwarten. Das finale Gesetz wird aufgrund der vielseitigen Wortbeiträge und den Vorschlägen von Bundesrat, Datenschützern, Digitalverbänden und Wirtschaft sicherlich noch einige Änderungen im Vergleich zum jetzt vorliegenden Regierungsentwurf aufweisen.

# Der Tragödie letzter Teil?

## Die Auswirkungen des Brexit auf Datenübermittlungen in das Vereinigte Königreich

*von Julius Nickoleit*

Nachdem sich die Briten am 24. Juli 2016 für einen Austritt aus der Europäischen Union entschieden haben, hält der sog. Brexit Europa in Atem. Ende des Jahres 2020 konnte das Schreckensszenarios des „Hard Brexit" in letzter Sekunde abgewendet werden. Das Vereinigte Königreich und die EU einigten sich auf das „Trade and Cooperation Agreement" (TCA), das die künftigen Beziehungen zwischen den Vertragsparteien regeln soll. Dieses betrifft natürlich auch Fragen des Datenschutzes, die hier näher beleuchtet werden sollen. Ist das TCA also der Schlussakt des politischen Dramas Brexit?

## I. Hintergrund

Die datenschutzrechtlich relevanten Fragen des Brexits entzünden sich vor allem am 5. Kapitel der Datenschutz-Grundverordnung (DSGVO). Dieses Kapitel enthält Regelungen für die Übermittlung personenbezogener Daten an Drittländer. Drittländer sind alle Staaten, die nicht Teil der EU oder des Europäischen Wirtschaftsraums (EWR) sind. Der Grundgedanke des 5. Kapitels der DSGVO ist es, eine Datenübermittlung in Drittstaaten nur zu erlauben, wenn sichergestellt werden kann, dass die betreffenden Drittstaaten einem im Wesentlichen zur DSGVO gleichwertigen Datenschutz bieten. So versucht die DSGVO einen Ausgleich zwischen dem wirtschaftlichen Interesse an einer Datenübermittlung und dem Schutz personenbezogener Daten auch außerhalb der Grenzen der EU sicherzustellen. Die DSGVO sieht verschiedene Möglichkeiten vor, durch die das gleichwertige Datenschutzniveau in einem Drittstaat sichergestellt werden kann (Art. 45-47 DSGVO). Ist keine dieser Möglichkeiten eröffnet, ist die Datenübermittlung unzulässig (Art. 44 DSGVO). Erfolgt sie dennoch, sind empfindliche Geldstrafen möglich (Art. 83 Abs. 5 lit. c) DSGVO). Die praktisch wichtigsten Instrumente zur Sicherstellung des gleichwertigen Datenschutzniveaus sind der Angemessenheitsbeschluss durch die Europäische Kommission (Art. 45 DSGVO) und der Einsatz von Standarddatenschutzklauseln (SCC) zwischen dem Verantwortlichen und dem Verarbeiter im Drittstaat (Art. 46 Abs. 2 lit. c) DSGVO). Liegen die Voraussetzungen dieser Normen vor, ist die Datenübermittlung zulässig.

Mit dem Austritt aus der EU würde das Vereinigte Königreich zu einem Drittstaat im Sinne der DSGVO werden, sodass auf Datenübermittlungen dorthin die Regelungen des 5. Kapitels der DSGVO anzuwenden wären. Folglich wären Datenübermittlungen nur unter den Voraussetzungen der Art. 45-47 DSGVO zulässig.

Der Austritt des Vereinigten Königreichs erfolgte am 31. Januar 2020. Die Beziehungen zwischen der EU und dem Vereinigten Königreich wurden dann zunächst durch das Brexit-Abkommen geregelt. Dieses sah vor, dass das Vereinigte Königreich bis zum 31. Dezember 2020 wie ein EU-Staat zu behandeln war. Es handelte sich daher auch nicht um einen Drittstaat im Sinne der DSGVO und die Regeln des 5. Kapitels der DSGVO fanden keine Anwendung. Datenübertragungen in das Vereinigte Königreich konnten unter den regulären Voraussetzungen der DSGVO stattfinden. Wie es nach dem 31. Dezember 2020 weitergehen sollte, war im Brexit-Abkommen aber nicht geregelt, weshalb bislang erhebliche Rechtsunsicherheit bestand.

## II. Regelungen im TCA

Zwar soll das TCA die Beziehungen zwischen der EU und dem Vereinigten Königreich nun langfristig regeln, gänzlich ausgeräumt wird die bisherige Rechtsunsicherheit durch das TCA jedoch nicht. Eine abschließende Regelung ist auch in ihm nicht enthalten. Vielmehr hat man sich auf die Vereinbarung eines weiteren Übergangszeitraums beschränkt und verschiedene vorstellbare Szenarien für den Ablauf dieses Zeitraums vorgesehen.

Der Übergangszeitraum betrifft alle Übermittlungen personenbezogener Daten in das Vereinigte Königreich ab dem 1. Januar 2021. Diese sind auch weiterhin nicht als Übermittlungen in ein Drittland zu betrachten. Es handelt sich um eine Fortsetzung des Übergangszeitraums, den das Brexit-Abkommen vorsah. Aktuelle Datenströme in das Vereinigte Königreich sind während des Übergangszeitraums also abgedeckt. Für sie sind nur die regulären Anforderungen der DSGVO zu beachten, das 5. Kapitel der DSGVO ist nicht anzuwenden. Das TCA sieht drei Szenarien vor, wie und wann dieser Übergangszeitraum endet. Sie werden im Folgenden dargestellt:

### 1. Erlass eines Angemessenheitsbeschlusses

Das erste Szenario ist der Erlass eines Angemessenheitsbeschlusses durch die Europäische Kommission. Der Angemessenheitsbeschluss ist wie bereits erörtert eine Möglichkeit, die Zulässigkeit von Datenübermittlungen in ein Drittland sicherzustellen (Art. 45 Abs. 1 DSGVO). Liegt ein solcher vor, sind Datenübermittlungen in das betreffende Drittland generell zulässig, Verantwortliche müssen lediglich die regulären Anforderungen der DSGVO beachten. Das TCA sieht nun vor, dass bei Erlass eines solchen Beschlusses der Übergangszeitraum automatisch endet. Das ist konsequent: wenn ein Angemessenheitsbeschluss vorliegt ist sichergestellt, dass Datenübermittlungen in das Vereinigte Königreich auch nach dem 5. Kapitel der DSGVO zulässig sind. Es besteht dann kein weiterer Bedarf für einen Übergangszeitraum. Ob ein solcher Angemessenheitsbeschluss in der näheren Zukunft realistisch zu erwarten ist, kann aber kaum mit Sicherheit gesagt werden. Angemessenheitsbeschlüsse bestehen momentan nur für die Schweiz, Argentinien und Japan, die jeweiligen Prüfungsverfahren dauerten teils Jahre an. Erleichtern könnte den Beschluss, dass in Großbritannien momentan eine nur leicht abgewandelte Version der DSGVO und der Data Protection Act 2018 gelten. Da die Rechtslage im Vereinigten Königreich mit der europäischen Rechtslage also fast identisch ist, könnte das einen Angemessenheitsbeschluss erleichtern. Andererseits könnte das Vereinigte Königreich die neu gewonnene Freiheit auch dazu nutzen, Zugriffsrechte von Geheimdiensten zu stärken. Das würde einem Angemessenheitsbeschluss im Weg stehen. Es ist somit zwar nicht ausgeschlossen, dass dieses Szenario eintritt, verlassen sollte man sich hierauf aber nicht.

### 2. Änderungen der Datenschutzgesetze im Vereinten Königreich

Das zweite Szenario ist eine Gesetzesänderung des Vereinigten Königreichs auf dem Gebiet des Datenschutzrechts. Diese Regelung ist in das TCA aufgenommen worden, um sicherzustellen, dass die aufgrund des Übergangszeitraums in das Vereinigte Königreich übermittelten Daten dort einen angemessenen Datenschutz genießen. Momentan gilt in Großbritannien wie gesehen ein beinahe identischer Datenschutz zur DSGVO. Sollte das Vereinigte Königreich diesen Datenschutz aber schon während des Übergangszeitraums lockern, endet konsequenterweise auch der Übergangszeitraum. Da in diesem Fall kein Angemessenheitsbeschluss der Kommission vorliegt, müssten Verantwortliche auf andere Möglichkeiten ausweichen, um die Zulässigkeit ihrer Datenübermittlungen sicherzustellen. Da das Ende des Übergangszeitraums vom Verhalten des Vereinigten Königreichs abhängt, kann dieses Szenario jederzeit eintreten. Datenübermittlungen in das Vereinigte Königreich könnten damit schlagartig unzulässig werden.

### 3. Zeitablauf

Das dritte Szenario ist das Ende des Übergangszeitraums durch Zeitablauf: der Übergangszeitraum endet nach vier Monaten und wird, falls keine Partei widerspricht, um weitere zwei Monate verlängert. Auch in diesem Fall besteht kein Angemessenheitsbeschluss der Kommission, sodass Verantwortliche auf andere Möglichkeiten ausweichen müssen.

In beiden Fällen des Ablaufs des Übergangszeitraums ohne einen Angemessenheitsbeschluss werden Verantwortliche im

Regelfall zu den SCCs nach Art. 46 Abs. 2 lit. c) DSGVO greifen. Es handelt sich hierbei um Vorlagen für Vertragsbedingungen, die beide Parteien einer Datenübermittlung vereinbaren und die den im Wesentlichen gleichwertigen Schutz zur DSGVO gewährleisten sollen. Im Unterschied zum Angemessenheitsbeschluss erlauben sie also nur die Übermittlung zu einem einzelnen Vertragspartner und müssen durch den Verantwortlichen selbst eingesetzt werden. Seit der Schrems-II Entscheidung des Europäischen Gerichtshofs (EuGH)[1] genügt es aber nicht mehr, die Klauseln einfach nur Vertragsbestandteil werden zu lassen. Darüber hinaus muss der Verantwortliche sicherstellen, dass ein angemessener Schutz der übertragenen Daten auch tatsächlich gewährleistet wird. Sollte das Vereinigte Königreich umfassende Zugriffsmöglichkeiten seiner Geheimdienste oder Ähnliches vorsehen, genügt die Verwendung der bisherigen SCCs allein also nicht.[2] Darüber hinaus muss der Verantwortliche zusätzliche Maßnahmen vorsehen, die die staatlichen Eingriffe kompensieren. Das könnten z. B. eine lokale Verschlüsselung oder Transportverschlüsselung sein oder die Verpflichtung des Datenimporteurs, bei Zugriffen durch Behörden des Vereinigten Königreichs gerichtlich gegen diese vorzugehen. Die Rechtsprechung des EuGH hierzu ist noch jung und es hat sich in der Praxis noch nicht herauskristallisiert, wie mit ihr umzugehen ist. Hier stellen sich also die gleichen Probleme wie im Verhältnis der EU zu den USA. Damit ist dieses Szenario zwar nicht wünschenswert, aber durchaus realistisch.

Das TCA ist somit keineswegs der Schlussstrich unter der langen Geschichte des Brexit. Vielmehr birgt es für die Zukunft erhebliche Unsicherheiten, die durch die Verunsicherungen über die SCCs durch den EuGH noch verstärkt werden.

## III. Fazit und Handlungshinweise für Hochschulen

Das wünschenswerteste Szenario ist der Erlass eines Angemessenheitsbeschlusses durch die Kommission. In diesem Fall können die Verantwortlichen der Universitäten und Forschungseinrichtungen Datenübermittlungen in das Vereinigte Königreich unproblematisch vornehmen, es sind lediglich die normalen Anforderungen der DSGVO zu beachten. Ergeht kein solcher Beschluss und endet der Übergangszeitraum nach Zeitablauf oder vielleicht sogar vorher sollte man jedoch vorbereitet sein. Ein erster Schritt ist die Analyse, an welchen Stellen Daten in das Vereinigte Königreich übermittelt werden. Hierbei kann es sich um die Benutzung von britischen Services, Datenverarbeitungs- oder Cloudprogrammen handeln, aber auch um die Kooperation mit britischen Universitäten oder Forschungseinrichtungen, in deren Rahmen personenbezogene Daten übertragen werden. Für diese Datenübermittlungen sollten entweder europäische Alternativen gesucht werden, oder es sollte sich – wo dies nicht möglich ist – darauf vorbereitet werden, die Datenübermittlung von nun an auf die Füße einer SCC zu stellen. Das kann unter Umständen auch weitergehende Garantien einschließen. Diesbezüglich sollte die weitere Entwicklung zu den SCCs und den Folgen des Schrems-II Urteils genauestens beobachtet werden.

1 Ausführlich hierzu: Uphues, Ins Wasser gefallen, DFN-Infobrief Recht 08/2020.

2 Siehe zu den Standarddatenschutzklauseln: Wellmann, O ihr gnadenbringenden Standarddatenschutzklauseln, DFN-Infobrief Recht 12/2020.

## 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