Kommunikation & Recht

Betriebs-Berater für
● Medien ● Telekommunikation ● Multimedia

1
K&R

25. Jahrgang Januar 2022 Seiten 1 – 72

dfv Mediengruppe · Frankfurt am Main

RAin Dr. Laura Schulte und wiss. Mitarbeiterin Christina Prowald*

Das neue Telekommunikation-Telemedien-Datenschutz-Gesetz

Anwendungsbereich und unionsrechtlicher Rahmen

Kurz und Knapp

Die Gesetzgebungsgeschichte des TTDSG veranschaulicht, wie komplex die Bestimmung datenschutzrechtlicher Anforderungen in digitalen Kontexten sein kann. Der Beitrag setzt sich mit dem rechtlichen Rahmen zur Bestimmung des geltenden Datenschutzrechts im Zusammenhang mit Telemedien und Telekommunikationsdiensten auseinander und überprüft anhand der Geltung des Fernmeldegeheimnisses bei der Privatnutzung betrieblicher Kommunikationsmittel sowie sog. PIMS, ob das TTDSG mehr Rechtssicherheit schafft.

I. Einleitung

Vielfach stellt sich in Online-Kontexten bereits die Bestimmung des anwendbaren Datenschutzrechts als anspruchsvolle Aufgabe dar; insoweit sind neben nationalen Rechtsvorschriften vor allem die des Unionsrechts zu beachten, welche die digitale Kommunikation zunehmend intensiver regulieren. Sowohl auf unionaler als auch auf mitgliedstaatlicher Ebene sind außerdem die Geltungsbereiche allgemeiner von spezielleren Rechtsakten abzugrenzen.

Im Folgenden werden zunächst die allgemeinen Grundsätze zur Bestimmung des Verhältnisses unterschiedlicher Normen am Beispiel des bereichsspezifischen Datenschutzrechts für die Telekommunikation und bei Telemedien aufgezeigt (II.). Anschließend wird der Anwendungsbereich des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (im Folgenden: TTDSG) konkretisiert (III.). Im Weiteren wird anhand zweier Beispiele – der Geltung des Fernmeldegeheimnisses für die Privatnutzung betrieblicher Kommunikationsmittel gestattende Arbeitgeber (IV. 1.) sowie der Regulierung von Personal-Information-Management-Systemen (im Folgenden: PIMS) (IV. 2.) – überprüft, ob mit dem TTDSG insoweit mehr Rechtssicherheit für Verbraucher, Diensteanbieter und Aufsichtsbehörden geschaffen wird.[1] Schließlich werden die Ergebnisse des Beitrags zusammengefasst (V.).

II. Bestimmung des anwendbaren Rechts im Mehrebenensystem

1. Allgemeine Grundsätze

Im Verhältnis zwischen dem europäischen und dem nationalen Recht ist zunächst der Anwendungsvorrang des Unionsrechts zu beachten.[2] Aus dem Vorrangprinzip folgt, dass im Falle eines Konflikts zwischen den Regelungen des nationalen und des europäischen Rechts die Bestimmungen des Unionsrechts vorrangig anzuwenden sind.[3] Dies gilt unabhängig von dem Rang der betroffenen mitgliedstaatlichen Regelung – als Verfassungs-, Bundes- oder Landesrecht – und deren Charakter – als Verfassung, Gesetz, Rechtsverordnung oder sog. Innenrecht.[4] Die unionalen Bestimmungen genießen dabei Anwendungsvorrang, jedoch keinen Geltungsvorrang.[5] Dies bedeutet, dass nationales Recht im Kollisionsfall nicht seine Gültigkeit verliert, sondern lediglich durch das Unionsrecht verdrängt wird.[6] In Konstellationen, in denen das Unionsrecht hingegen nicht tangiert wird, kommt die nationale Regelung weiterhin zur Anwendung.

Nach dem Grundsatz „lex specialis derogat legi generali" (Spezialitätsgrundsatz), der sowohl auf unionaler als auch auf mitgliedstaatlicher Ebene gilt, verdrängt eine speziellere Norm die allgemeinere Norm.[7] Die Spezialität eines Rechtsaktes kann sich allgemein aus dessen Anwendungsbereich, aber auch aus dessen einzelnen Normen ergeben.[8] Im Hinblick auf das Verhältnis zwischen unionalem und nationalem Recht ist jedoch zu berücksichtigen, dass eine speziellere nationale Bestimmung eine unionale Regelung nur dann verdrängt, wenn und soweit der unionale Rechtsakt dies auch zulässt, insbesondere im Rahmen sog. Öffnungsklauseln, siehe z. B. Art. 88 DSGVO.

Der Grundsatz „lex posterior derogat legi priori" besagt, dass eine aktuellere Norm einer bereits zuvor in Kraft getretenen Norm vorgeht. Auch diese Regel gilt sowohl im nationalen Recht als auch im Unionsrecht.[9] Allerdings geht der Anwendungsvorrang auch diesem Grundsatz vor; eine unionale Bestimmung geht im Verhältnis zu einer zu einem späteren Zeitpunkt erlassenen nationalen Regelung in ihrem Anwendungsbereich im Zweifel vor.[10]

Bei der Anwendung nationaler Rechtsakte, die der Umsetzung europäischer Richtlinien dienen, ist darüber hinaus der Grundsatz der richtlinienkonformen Auslegung zu berücksichtigen. Dieser verlangt, dass bei der Auslegung entsprechender nationaler Bestimmungen ein etwaig bestehender Beurteilungsspielraum weitestmöglich auszunutzen ist, um die Rechtsanwendung so nah wie möglich an Sinn und Zweck der jeweiligen Richtlinie auszurich-

* Mehr über die Autorinnen erfahren Sie am Ende des Beitrags. Alle zitierten Internetquellen wurden zuletzt abgerufen am 5. 12. 2021.

1 BT-Drs. 19/27441, S. 30.

2 Hierzu EuGH, 15. 7. 1964 – 6/64, NJW 1964, 2371 – Costa / E.N.E.L.

3 *Conrad*, in: Auer-Reinsdorff/Conrad (Hrsg.), Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 34 Rn. 16.

4 *Conrad*, in: Auer-Reinsdorff/Conrad (Fn. 3), § 34 Rn. 16.

5 *Kugelmann*, in: ders. (Hrsg.), Landesdatenschutzgesetz Rheinland-Pfalz, § 1 Rn. 21.

6 *Kugelmann*, in: ders. (Fn. 5), § 1 Rn. 21.

7 *Saria*, in: Liebscher/Flohr/Petsche, Handbuch der EU-Gruppenfreistellungsverordnungen, 2. Aufl. 2012, § 3 Rn. 27.

8 *Eikenberg*, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der EU, 73. EL Mai 2021, AEUV, Art. 182 Rn. 86.

9 *Saria*, in: Liebscher/Flohr/Petsche (Fn. 7), § 3 Rn. 27.

10 *Geismann*, in: von der Groeben/Schwarze/Hatje (Hrsg.), Europäisches Unionsrecht, 7. Aufl. 2015, AEUV, Art. 288 Rn. 8.

ten.[11] Dies kann unter Umständen auch eine Fortbildung des nationalen Rechts bedingen.[12]

2. Verhältnis von DSGVO, E-Privacy-RL, E-Privacy-VO und TTDSG

Die DSGVO gilt als Verordnung gem. Art. 288 Abs. 2 AEUV unmittelbar in jedem Mitgliedstaat, sie bedarf damit keiner Transformation in nationales Recht und enthält den „Allgemeinen Teil" des unionsweit geltenden Datenschutzrechts. Dem Charakter einer *Grund*verordnung entsprechend ist die DSGVO in vielen Teilen so abstrakt formuliert, dass sie der Konkretisierung durch weitere Rechtsakte sowohl auf horizontaler als auch auf vertikaler Ebene bedarf.[13] Auf unionaler Ebene können dies etwa Durchführungsbeschlüsse sein. In der Vergangenheit wurden Durchführungsbeschlüsse insbesondere im Zusammenhang mit der Anerkennung des Datenschutzniveaus in Drittstaaten als „angemessen" gefasst, vgl. Art. 45 Abs. 3 DSGVO.[14] Auf nationaler Ebene ist insoweit insbesondere der Spielraum zu nutzen, den die Öffnungsklauseln der DSGVO ausdrücklich vermitteln.[15]

Die E-Privacy-RL enthält datenschutzrechtliche Vorgaben für den Bereich der elektronischen Kommunikation. Diese Richtlinie ist insoweit der im Verhältnis zur DSGVO speziellere Rechtsakt und geht dieser diesbezüglich vor. Erwägungsgrund 10 der E-Privacy-RL stellt allerdings klar, dass der RL 95/46/EG bzw. nunmehr der DSGVO auch im Bereich der elektronischen Kommunikation ein Anwendungsbereich bezüglich aller Fragen des Schutzes der Grundrechte und Grundfreiheiten, die von der E-Privacy-RL nicht spezifisch erfasst werden, einschließlich der Pflichten des für die Verarbeitung Verantwortlichen und der Betroffenenrechte, verbleibt. Neben „rein datenschutzrechtlichen" Aspekten enthält die E-Privacy-RL auch Regelungen zur Vertraulichkeit der Kommunikation und zum Schutz von Informationen auf Endgeräten, unabhängig davon, ob es sich insoweit um personenbezogene Daten handelt.

Im Gegensatz zu einer Verordnung gilt eine Richtlinie nicht unmittelbar, sondern muss eine solche von den Mitgliedstaaten erst in nationales Recht umgesetzt werden, vgl. Art. 288 Abs. 3 AEUV, es sei denn, der nationale Gesetzgeber kommt seiner Umsetzungspflicht nicht fristgerecht nach und die Bestimmungen der Richtlinie sind uneingeschränkt, hinreichend klar und eindeutig.[16] In Anbetracht dessen, dass der E-Privacy-RL keine vollharmonisierende Wirkung zukommt, kann der nationale Gesetzgeber im Rahmen ihrer Umsetzung dort, wo die Richtlinie selbst keine abschließenden Regelungen enthält, grundsätzlich Regelungen, die über das Schutzniveau der Richtlinie hinausgehen, erlassen.[17] Solche „überschießenden" Regelungen müssen allerdings auch den sonstigen Vorgaben des Unionsrechts – insbesondere der DSGVO – hinreichend Rechnung tragen. Eine Unterschreitung des Schutzniveaus, das durch die E-Privacy-RL gewährt wird, ist ausgeschlossen.[18] Im Ergebnis gehen die nationalen Regelungen, die die E-Privacy-RL richtlinienkonform umsetzen, der DSGVO als speziellere Vorschriften vor, vgl. Art. 95 DSGVO.

Das TTDSG dient vor allem der ausdrücklichen Anpassung des deutschen Datenschutzrechts an die Vorgaben der E-Privacy-RL und der DSGVO.[19] Hintergrund für das Tätigwerden des deutschen Gesetzgebers war insoweit die Europarechtswidrigkeit einiger datenschutzrechtlicher Regelungen des Telemediengesetzes (im Folgenden: TMG) aufgrund der Tatsache, dass die betreffenden Bestimmungen weder durch eine Öffnungsklausel der DSGVO noch durch den Umsetzungsspielraum der E-Privacy-RL gedeckt waren.[20] Soweit das TTDSG die E-Privacy-RL richtlinienkonform umsetzt, gehen dessen Regelungen der DSGVO vor.

Der europäische Gesetzgeber arbeitet bereits seit geraumer Zeit an einer E-Privacy-VO, welche die E-Privacy-RL ablösen und die rechtlichen Vorgaben (auch) insoweit vollharmonisieren soll. Wann die E-Privacy-VO, die ursprünglich gemeinsam mit der DSGVO in Kraft treten sollte, erlassen wird, ist derzeit noch offen. Sollte die E-Privacy-VO in Kraft treten, ist sie nach Art. 288 AEUV in all ihren Teilen verbindlich und gilt unmittelbar. Der Erlass von nationalen Regelungen in ihrem Anwendungsbereich wird sodann nur noch in den Bereichen möglich sein, in denen die Verordnung dies selbst vorsieht, insbesondere im Rahmen von Öffnungsklauseln. Im Ergebnis bedeutet dies, dass das Inkrafttreten der E-Privacy-VO – je nach ihrer konkreten Ausgestaltung – die Nichtanwendung des TTDSG bedingen kann.

III. Anwendungsbereich des TTDSG

1. Sachlicher Anwendungsbereich

a) Datenschutz vs. Fernmeldegeheimnis

Der sachliche Anwendungsbereich des TTDSG wird in § 1 des Gesetzes geregelt. Das Gesetz soll insbesondere den Schutz der Privatsphäre bei der Nutzung von Telemedien wie auch von Telekommunikationsdiensten sicherstellen, vgl. § 1 Abs. 1 Nr. 2 TTDSG. Das bereichsspezifische Datenschutzrecht im Telekommunikationssektor, dem u. a. die Anbieter bestimmter Telekommunikationsdienste unterliegen, dient dem Schutz des Fernmeldegeheimnisses, das auch als Telekommunikationsgeheimnis bezeichnet wird, vgl. § 1 Abs. 1 Nr. 1 TTDSG. Das Fernmeldegeheimnis soll Kommunikationsteilnehmer vor einem unkontrollierten Zugriff Dritter auf die erst mittels einer bestimmten Übertragungstechnik, die sich nur bedingt unter der Kontrolle der Kommunikationsteilnehmer selbst befindet, ermöglichten Kommunikation schützen.

Dem Fernmeldegeheimnis unterliegen sowohl der Inhalt von Telekommunikation als auch ihre näheren Umstände. Ihre näheren Umstände bilden etwa Informationen über Beginn, Ende und Dauer der Kommunikation sowie erfolglose Verbindungsversuche.[21] Fernmeldegeheimnis und Datenschutz haben grundsätzlich eine verhältnismäßig große Überlappung ihres Schutzgegenstandes, denn oftmals sind Telekommunikationsinhalte und -umstände personenbezogene Daten. Zu berücksichtigen sind jedoch insbesondere zwei Abweichungen des Schutzumfangs beider Rechte:

11 EuGH, 13. 11. 1990 – C-106/89, DB 1991, 157 – Marleasing; EuGH, 14. 3. 1996 – C-168/95, BB 1996, 973 – Arcaro.
12 BGH, 28. 5. 2020 – I ZR 7/16, K&R 2020, 611 – Cookie II.
13 *Schulte*, Vom quantitativen zum qualitativen Datenschutz, 2018, S. 238.
14 Hierzu *Meyer/Schulte*, in: Pachinger (Hrsg.), Datenschutz – Recht und Praxis, 2019, 8.3. Rn. 20.
15 *Schulte* (Fn. 13), S. 238.
16 *Schroeder*, in: Streinz (Hrsg.), EUV/AEUV, 3. Aufl. 2018, AEUV, Art. 288 Rn. 91.
17 *Remien*, in: Schulze/Janssen/Kadelbach (Hrsg.), Europarecht, 4. Aufl. 2020, § 14 Rn. 43.
18 *Magnus*, in: Grabitz/Hilf (Hrsg.), Das Recht der Europäischen Union, 40. Aufl. 2009, Richtlinie 1999/44/EG, Vorb. vor Art. 1 Rn. 13.
19 BT-Drs. 19/27441 S. 1.
20 Hierzu *Assion*, Ausschussdrucksache 19(9)1039, S. 1.
21 Zum verfassungsrechtlichen Fernmeldegeheimnis *Gusy*, in: von Mangoldt/Klein/Starck (Hrsg.), GG, 7. Aufl. 2018, Art. 10 Rn. 50 ff.

– Personelle Dimension: Im Gegensatz zum Datenschutz unterliegen dem Fernmeldegeheimnis auch Einzelangaben über (zumindest bestimmbare) juristische Personen bzw. rechtsfähige Personengesellschaften, vgl. § 1 Abs. 2 TTDSG.
– Zeitliche Dimension: Von dem Fernmeldegeheimnis werden Informationen geschützt, die während einer laufenden Kommunikation anfallen. Ob bzw. inwieweit das Fernmeldegeheimnis seinen Schutz auch nach dem Ende eines Kommunikationsvorgangs entfaltet, ist umstritten.[22] Der Schutz, den das Datenschutzrecht vermittelt, besteht unabhängig von einem Kommunikationsvorgang.

Die bereichsspezifischen Datenschutzregelungen, die für Telekommunikationsvorgänge gelten, haben vor den allgemeinen datenschutzrechtlichen Vorgaben Vorrang, wenn und soweit sie der Umsetzung der E-Privacy-RL dienen, vgl. Art. 95 DSGVO.[23] Die §§ 9 bis 13 TTDSG haben damit im Zweifel Vorrang vor der DSGVO – jedoch nur, wenn und soweit sie anwendbar sind, also vor allem im Verhältnis zu Anbietern von öffentlich zugänglichen Telekommunikationsdiensten.

b) OTT-Dienste

Sog. Over-the-Top-Dienste (im Folgenden: OTT-Dienste) sind Kommunikationsdienste, die über das Internet erbracht werden. Die unterschiedlichen OTT-Dienste lassen sich wie folgt systematisieren:[24]

– OTT-0-Dienste: Teilweise über das Internet erbrachte Kommunikationsdienste, i. d. R. nummerngebundene interpersonelle Kommunikationsdienste. Z. B. Skype-Out.
– OTT-1-Dienste: Ausschließlich über das Internet erbrachte Kommunikationsdienste, i. d. R. nicht-nummerngebundene Kommunikationsdienste. Z. B. WhatsApp und Signal.
– OTT-2-Dienste: Über das Internet erbrachte Inhaltsdienste. Z. B. Soziale Netzwerke.

Das Telekommunikationsdatenschutzrecht des TTDSG knüpft sachlich an Telekommunikationsdienste an. Mit dem Telekommunikationsmodernisierungsgesetz, das der Umsetzung des europäischen Kodex für die elektronische Kommunikation dient und parallel zum TTDSG in Kraft tritt, wurde der Begriff der Telekommunikationsdienste erweitert. Während diese nach § 3 Nr. 24 TKG-alt als i. d. R. gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, definiert wurden, bilden Telekommunikationsdienste nach § 3 Nr. 61 TKG-neu nunmehr i. d. R. gegen Entgelt über Telekommunikationsnetze erbrachte Dienste, die folgende Dienste umfassen:

– Internetzugangsdienste,
– interpersonelle Telekommunikationsdienste und
– Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie Übertragungsdienste, die für Maschine-Maschine-Kommunikation und für Rundfunk genutzt werden.

Interpersonelle Telekommunikationsdienste werden in § 3 Nr. 24 TKG-neu wiederum als solche Telekommunikationsdienste bezeichnet, die

– gewöhnlich gegen Entgelt erbracht werden,
– einen direkten interpersonellen und interaktiven Informationsaustausch über Telekommunikationsnetze
– zwischen einer endlichen Zahl von Personen ermöglichen,
– wobei die Empfänger von den Personen bestimmt werden, die die Telekommunikation veranlasst haben oder daran beteiligt sind,
– mit Ausnahme solcher Dienste, die eine interpersonelle und interaktive Telekommunikation lediglich als untrennbar mit einem anderen Dienst verbundene Nebenfunktion ermöglichen.[25]

Bis zum Inkrafttreten des Telekommunikationsmodernisierungsgesetzes galten lediglich OTT-0-Dienste als Telekommunikationsdienste im Sinne des TKG und unterlagen damit lediglich solche Dienste den Regelungen der §§ 88 ff. TKG-alt.[26] Demgegenüber galten OTT-1-Dienste, mit denen zwar Inhalte über das Internet ausgetauscht werden können, die aber selbst keine Übertragung von Signalen zu diesem Zweck vornehmen, nicht als Telekommunikationsdienste. Da die Definition für interpersonelle Kommunikationsdienste – in Umsetzung von Art. 2 Nr. 4 lit. b und Nr. 5 des europäischen Kodex für die elektronische Kommunikation – die Übertragung von Signalen nicht mehr voraussetzt, bilden nunmehr auch Messenger-Dienste wie WhatsApp und Signal Telekommunikationsdienste i. S. d. TKG und finden damit die Bestimmungen des TTDSG Anwendung auf diese, § 2 Abs. 1 TTDSG.[27]

2. Personeller und örtlicher Anwendungsbereich

Der personelle sowie der örtliche Anwendungsbereich des TTDSG ergeben sich ebenfalls aus § 1 TTDSG. Nach § 1 Abs. 3 S. 1 TTDSG unterliegen alle Unternehmen und Personen, die im Geltungsbereich des TTDSG über eine Niederlassung verfügen oder Dienstleistungen erbringen oder auch nur daran mitwirken oder Waren auf dem Markt bereitstellen, den Regelungen des TTDSG.[28] Anknüpfungspunkte für eine Anwendbarkeit des TTDSG sind entsprechend zum einen das Erbringen einer Leistung bzw. die Mitwirkung an einer solchen sowie zum anderen der Ort der Bereitstellung einer Leistung.

Dadurch, dass bereits ein Mitwirken an der Leistung für die Geltung des TTDSG ausreichend sein soll, wird der Anwendungsbereich des Gesetzes in personeller Hinsicht verhältnismäßig weit gefasst. Zu den verpflichteten Personen gehören neben den eigentlichen Anbietern von Telemedien und Telekommunikationsdiensten auch deren Dienstleister, ohne dass diese zwingend an der inhaltlichen Ausgestaltung der Leistung, die durch das TTDSG reguliert werden soll, beteiligt sein müssen.[29] Entsprechend können beispielsweise Hosting-Dienstleister bzw. Cloud-Anbieter vom Anwendungsbereich des Gesetzes erfasst werden, ohne dass diese selbst eine Möglichkeit zur (gesetzeskonformen) Ausgestaltung des angebotenen Diens-

22 Für ein Ende des Schutzes ab dem Ende des Übertragungsvorgangs BVerfG, 2. 3. 2006 – 2 BvR 2099/04, K&R 2006, 178.
23 Hierzu auch European Data Protection Board, Opinion 5/2019, abrufbar unter: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en.
24 BEREC, Report on OTT services, BoR (16) 35 vom 29. 1. 2006, abrufbar unter: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services.
25 Im Weiteren differenziert das TKG noch zwischen nummerngebundenen (§ 3 Nr. 37 TKG-neu) und nummernunabhängigen interpersonellen Kommunikationsdiensten (§ 3 Nr. 40 TKG-neu).
26 EuGH, 5. 6. 2019 – C-142/18, K&R 2019, 484 – SkypeOut.
27 Zuvor hatte der EuGH noch entschieden, dass der von Google angebotene E-Mail-Dienst Gmail kein Telekommunikationsdienst sei: EuGH, 13. 6. 2019 – C-193/18, K&R 2019, 487 – Gmail.
28 Hinsichtlich der Erfassung von OTT-Diensten siehe III. 1. b).
29 *Golland*, Ausschussdrucksache 19(9)1054, S. 3.

tes haben. Berücksichtigt man außerdem die Definition des „Anbieters von Telemedien" nach § 2 Abs. 2 Nr. 1 TTDSG, werden konsequenterweise auch die jeweiligen Mitarbeiter der Anbieter direkt vom Anwendungsbereich des Gesetzes erfasst.[30]

Außerdem bedingt die Anknüpfung an den Ort der Leistungserbringung bzw. das Marktortprinzip den weiten Geltungsanspruch des Gesetzes, vgl. § 1 Abs. 3 S. 1 TTDSG.[31] Das Marktortprinzip, das in Art. 3 Abs. 2 DSGVO normiert ist, bezieht den Anwendungsbereich datenschutzrechtlicher Vorgaben auch auf alle datenverarbeitenden Stellen außerhalb der EU, sofern sich deren Leistungen bzw. Angebote auch an Betroffene in der EU richten. Eines Sitzes oder einer Niederlassung innerhalb der EU bedarf es hingegen gerade nicht.[32] Überträgt man das Marktortprinzip auf das TTDSG, führt dies dazu, dass Diensteanbieter außerhalb Deutschlands – und letztlich auch deren Mitarbeiter – vom Anwendungsbereich des TTDSG grundsätzlich erfasst werden, soweit sie ihre Leistungen auf dem deutschen Markt anbieten. Fraglich bleibt insoweit jedoch, wie das TTDSG gegenüber diesen Unternehmen vollzogen werden soll. Insoweit fehlt es nämlich an entsprechenden Regelungen und Mechanismen, die insbesondere die Zusammenarbeit von Aufsichtsbehörden koordinieren.

§ 1 Abs. 3 S. 2 TTDSG regelt weiter, dass § 3 des TMG auch bei der Anwendung des TTDSG zu berücksichtigen ist. Soweit sich die Bestimmungen des TTDSG auf Telemedien beziehen, ist somit grundsätzlich das in § 3 TMG normierte Herkunftslandprinzip zu berücksichtigen. Das Herkunftslandprinzip besagt, dass Dienstanbieter auch im Falle der Erbringung ihrer Leistungen in einem anderen Mitgliedstaat der EU als demjenigen, in dem sich ihr Sitz befindet, im Zweifelsfall den rechtlichen Bestimmungen ihres Herkunftsstaates unterliegen.[33] Das Prinzip gilt allerdings nur für den innereuropäischen Bereich und soll hier den freien Dienstleistungsverkehr sicherstellen, Dienstleister aus Drittstaaten werden hingegen von diesem gerade nicht erfasst.[34] In Anbetracht dessen, dass die europäischen Datenschutzregelungen in allen Mitgliedstaaten grundsätzlich ein gleichwertiges Datenschutzniveau sicherstellen sollen, während ein solches in Drittstaaten gerade nicht ohne Weiteres vermutet werden kann, ist eine solche Differenzierung durchaus nachvollziehbar. Allerdings hat der Gesetzgeber des TTDSG die Frage, welche Konsequenzen aus § 3 Abs. 2 Nr. 4 TMG resultieren, demzufolge das Herkunftslandprinzip das geltende Datenschutzrecht unberührt lässt, unberücksichtigt gelassen. Im Ergebnis dürfte es aus Gründen der Vorsicht damit auch für europäische Anbieter weiterhin erforderlich sein, die datenschutzrechtlichen Besonderheiten sowie die aufsichtsbehördliche Praxis in jedem Mitgliedstaat der Union zu berücksichtigen, in dem sie Telemedien anbieten.

IV. Ausgewählte Regelungsaspekte

1. Geschäftsmäßiges Anbieten von Telekommunikationsdiensten

Während der Referentenentwurf des TTDSG in der Fassung vom 12. 1. 2021 noch vorsah, dass (lediglich) die Anbieter öffentlich zugänglicher Telekommunikationsdienste und Betreiber öffentlicher Kommunikationsnetze zur Wahrung des Fernmeldegeheimnisses verpflichtet sein sollten,[35] wurde der Kreis der durch das Fernmeldegeheimnis Verpflichteten letztlich wesentlich erweitert. Laut § 3 Abs. 2 S. 1 Nr. 2 TTDSG sind nunmehr auch Anbieter von „ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken" zur Wahrung des Fernmeldegeheimnisses verpflichtet.

Obwohl der Begriff „Geschäftsmäßigkeit" im Telekommunikationsrecht nicht legal-definiert ist, wird hierunter überwiegend die Schaffung eines nachhaltigen Angebots und dies unabhängig von dem Vorliegen einer Gewinnerzielungsabsicht verstanden.[36] Im Ergebnis führt dieses weite Begriffsverständnis dazu, dass Arbeitgeber bereits dann als geschäftsmäßige Anbieter von Telekommunikationsdiensten zu qualifizieren sein dürften, wenn sie die Privatnutzung betrieblicher Kommunikationsmittel wie etwa Smartphones und E-Mail-Accounts erlauben bzw. dulden und somit diese ihren Mitarbeitern nachhaltig zur Verfügung stellen. Unter Berücksichtigung dieser Definition haben solche Arbeitgeber das Fernmeldegeheimnis bzw. die speziellen Datenschutzvorschriften des 2. Teils des TTDSG – also die §§ 9 bis 13 TTDSG – zu beachten. Daneben kann die Geltung des Fernmeldegeheimnisses auch strafrechtliche Relevanz entfalten, vgl. § 206 StGB.

Soweit eine Bestimmung auf nationaler Ebene der Umsetzung der E-Privacy-RL dient, die Verarbeitung personenbezogener Daten regelt und im Verhältnis zu der E-Privacy-RL eine „überschießende Tendenz" entfaltet, ist diese Bestimmung nicht anzuwenden, wenn der Anwendungsvorrang der DSGVO insoweit Relevanz entfaltet.[37] Denn die DSGVO wird durch einen mitgliedsstaatlichen Rechtsakt nur dann „verdrängt", wenn die DSGVO dies selbst – insbesondere im Rahmen von Öffnungsklauseln – vorsieht. Aufgrund von § 3 Abs. 2 S. 1 Nr. 2 TTDSG können allerdings keine spezielleren Vorschriften zur DSGVO formuliert werden, soweit diese über die Vorgaben der E-Privacy-RL hinausgehen und damit selbst keine in der E-Privacy-RL festgelegten Pflichten darstellen, vgl. Art. 95 DSGVO.

§ 3 TTDSG dient der Umsetzung von Art. 5 Abs. 1 E-Privacy-RL, der die Mitgliedstaaten (ausschließlich) dazu verpflichtet, die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten sowie der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicherzustellen. Das Kriterium der Geschäftsmäßigkeit sieht die umzusetzende europäische Vorgabe hingegen nicht vor. Auch der europäische Kodex für die elektronische Kommunikation kennt das Kriterium der Geschäftsmäßigkeit nicht, dieser stellt demgegenüber auf das Kriterium der Entgeltlichkeit im Sinne einer konkreten Gegenleistung für die Bereitstellung eines Kommunikationsdienstes ab.[38] Zwar heißt es in Anerkennung des Kodex in der Begründung des Regierungsentwurfs des TTDSG „Klarstellend sei darauf hingewiesen, dass Telekommunikationsdienste entsprechend der Begriffsbestimmung der

30 *Golland*, Ausschussdrucksache 19(9)1054, S. 3.
31 BT-Drs. 19/27441, S. 34.
32 EuGH, 13. 5. 2014 – C-131/12, K&R 2014, 378 – Google Spain.
33 *Nordmeier*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 4. Aufl. 2019, TMG, § 3 Rn. 12.
34 *Nordmeier*, in: Spindler/Schuster (Fn. 33), TMG, § 3 Rn. 8.
35 Siehe § 3 Abs. 2 S. 1 TTDSG-E, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Artikel/Service/Gesetzesvorhaben/gesetz-zur-regelung-des-datenschutzes-und-des-schutzes-privatsphaere.html.
36 So etwa BT-Drs. 14/6098, S. 17.
37 Zu dem gleichen Ergebnis kommend *Schwartmann*, Ausschussdrucksache 19(9)1043, S. 10 f.; s. a. *Kühling/Sauerborn*, CR 2021, 271, 273 f.
38 Zur Definition des Kriteriums „entgeltlich" EuGH, 22. 5. 2003 – C-355/00, BeckRS 2004, 76684 – Freskot.

RL (EU) 2018/1972 und damit des nationalen Telekommunikationsrechts nur solche sind, die in der Regel gegen Entgelt erbracht werden",[39] allerdings bildet die Definition des § 3 Abs. 2 S. 1 Nr. 2 TTDSG dieses Verständnis nicht ab.

Art. 3 Abs. 1 der E-Privacy-RL bestimmt, dass diese für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft gilt. Bei betrieblichen Kommunikationsmitteln handelt es sich jedoch nicht um öffentliche Kommunikationsmittel in dem Sinne, dass diese allen Mitgliedern der Öffentlichkeit auf der gleichen Grundlage zugänglich wären. Die Gefährdungslage im Verhältnis zum Arbeitgeber dürfte sich auch grundsätzlich nicht als mit der gegenüber den Anbietern öffentlicher Kommunikationsdienste vergleichbar darstellen. Außerdem ist bei einer strikten Anwendung der DSGVO und gerade nicht des TTDSG nicht von einer Schutzlücke zulasten der betroffenen Angestellten auszugehen. Schließlich steht die Erstreckung des Fernmeldegeheimnisses in der zuvor dargestellten Weise im Widerspruch zu dem Ziel der Harmonisierung, soweit das Kriterium der Geschäftsmäßigkeit den Umsetzungsakten in anderen Mitgliedstaaten fremd ist.

Zusammenfassend dürfte damit aufgrund des Anwendungsvorrangs des Unionsrechts davon auszugehen sein, dass sich die Privatnutzung gestattende Arbeitgeber auch weiterhin (lediglich) an den Vorgaben der DSGVO zu orientieren haben. Außerdem wird an der hier diskutierten Frage der Geschäftsmäßigkeit von erbrachten Telekommunikationsdiensten deutlich, dass die beiden Gesetzesinitiativen, die zum Erlass des TTDSG und des Telekommunikationsmodernisierungsgesetzes geführt haben, partiell nicht hinreichend abgestimmt wurden, denn im Rahmen des TKG hat der Bundesgesetzgeber das Kriterium der Geschäftsmäßigkeit gestrichen, vgl. noch § 3 Nr. 6 TKG-alt.

2. Personal Information Management-Systeme

§ 26 TTDSG sieht nun erstmals eine Regelung für Dienste zur Einwilligungsverwaltung – sog. Personal-Information-Management-Systeme – im nationalen Recht vor. Eine entsprechende Bestimmung fand sich bereits ursprünglich im Referentenentwurf des TTDSG, wurde im Laufe des Gesetzgebungsverfahrens gestrichen und hat nun doch Eingang in die endgültige Fassung des TTDSG gefunden.

Hintergrund der Einführung dieser Regelung ist das in Art. 5 Abs. 3 E-Privacy-RL normierte Einwilligungserfordernis im Hinblick auf die Speicherung und Auswertung von Informationen in bzw. aus den Endeinrichtungen von Nutzern, insbesondere mittels sog. Cookies oder diesen vergleichbaren Technologien.[40] Die E-Privacy-RL statuiert damit das „Ob" der Einwilligungspflicht in entsprechende Datenverarbeitungsprozesse, die DSGVO hingegen das „Wie" der Einwilligung. Die Anforderungen, die aus dem Einwilligungserfordernis resultieren, sind durch den EuGH u. a. in seiner Entscheidung Planet49 jüngst konkretisiert worden.[41] In Anerkennung dieser Rechtsprechung entschied der BGH konsequenterweise, dass § 15 Abs. 3 TMG-alt richtlinienkonform dahingehend auszulegen bzw. fortzubilden sei, dass der Einsatz von Cookies, die technisch nicht zwingend erforderlich sind, das Vorliegen einer informierten und aktiven Einwilligung der Betroffenen erfordere und eine bloße Opt-Out-Möglichkeit den europarechtlichen Anforderungen hingegen gerade nicht genüge.[42] § 25 TTDSG greift diese Rechtsprechung auf und soll nun (endlich) die Vorgaben der E-Privacy-RL insoweit umsetzen.

Neben einer eindeutigen Willensbekundung oder anderen bestätigenden Handlung setzt eine wirksame Einwilligung nach Art. 4 Nr. 11 DSGVO voraus, dass diese freiwillig, für den konkreten Fall und in informierter Weise durch die betroffene Person abgegeben wird.[43] Der hinter dem Einwilligungserfordernis stehende Gedanke, dass der Nutzer basierend auf den ihm transparent zur Verfügung gestellten Informationen selbstbestimmt über die Erhebung und Verwendung seiner Daten entscheiden können soll, ist vom Grundsatz her zu begrüßen. Dieser Ansatz hat allerdings in der Praxis dazu geführt, dass Nutzer nahezu auf jeder Website mit einer Einwilligungsabfrage sowie umfangreichen Informationen über Analyse- bzw. Marketing-Tools konfrontiert werden, da entsprechende Anwendungen bei der Mehrzahl von Internetpräsenzen zum Einsatz kommen. Dabei sind die Einwilligungsabfragen häufig so ausgestaltet, dass sie den Nutzer durch eine „geschickte" Gestaltung in seiner Entscheidung lenken oder Schaltflächen zur Ablehnung von Cookies bisweilen gar nicht funktionieren. Soweit dies dazu führt, dass Nutzer die Einwilligungsabfragen lediglich als lästiges Hindernis wahrnehmen, die bereitgestellten Informationen nicht zur Kenntnis nehmen und Consent-Banner möglichst schnell weggeklickt werden, wird der eigentliche Zweck des Einwilligungserfordernisses konterkariert.[44]

Dieser Problematik will der Bundesgesetzgeber nun durch die Regulierung von PIMS begegnen und dem Nutzer so die Konfrontation mit einer Vielzahl partiell unübersichtlicher Einwilligungsprozesse ersparen.[45] Mittels PIMS soll Nutzern die Möglichkeit gegeben werden, innerhalb einer Benutzeroberfläche Informationen über gem. § 25 TTDSG einwilligungspflichtige Datenverarbeitungsprozesse abzurufen und seine Einwilligungen insoweit zu verwalten.[46] So soll die Auseinandersetzung des Nutzers mit den hier relevanten datenschutzrechtlichen Fragestellungen gefördert werden, da der Nutzer die Einstellungen unabhängig von dem Wunsch nach dem Aufruf einer bestimmten Anwendung vornehmen kann.[47] Unter diesem Gesichtspunkt ist die Einführung einer transparenten Verwaltungsmöglichkeit grundsätzlich zu begrüßen, das Konzept wirft jedoch auch einige Fragen bzw. Probleme auf.

Insbesondere stellt sich die Frage, inwieweit die Regelung einer solchen Einwilligungsverwaltung überhaupt von den Kompetenzen des Bundesgesetzgebers gedeckt ist. Der Gestaltungsspielraum des nationalen Gesetzgebers auf dem Gebiet des Datenschutzrechts ist verhältnismäßig stark beschränkt. Die Einwilligungspflichtigkeit im Hinblick auf den Einsatz technisch nicht zwingend erforderlicher Cookies und diesen vergleichbaren Technologien wird durch die E-Privacy-RL geregelt. Aus Erwägungsgrund 66 der RL 2009/136/EG ergibt sich, dass Einwilli-

39 BT-Drs. 19/27441, S. 34.
40 *Schwartmann/Hanloser/Weiß*, Kurzgutachten PIMS im TTDSG, März 2021, S. 2, abrufbar unter: https://enid.foundation/wp-content/uploads/2021/03/Schwartmann_Hanloser_Weiss-Kurzgutachten_Dienste_zur_Einwilligungsverwaltung_20210302.pdf.
41 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 – Planet49.
42 BGH, 28. 5. 2020 – I ZR 7/16, K&R 2020, 611 – Cookie II.
43 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 – Planet49.
44 *Schwartmann/Hanloser/Weiß* (Fn. 40), S. 2.
45 *Richter*, Ausschussdrucksache 19(9)1045, S. 2.
46 *Engeler*, Ausschussdrucksache 19(9)1056, S. 3; *Schwartmann/Hanloser/Weiß* (Fn. 40), S. 2.
47 *Assion*, Ausschussdrucksache 19(9)1039, S. 10.

gungen, die die Speicherung von Informationen auf einer Endeinrichtung des Nutzers betreffen, auch mittels entsprechender Einstellungen eines Browsers oder mittels einer anderen Anwendung eingeholt werden können, soweit dies in Einklang mit der RL 95/46/EG bzw. der DSGVO geschieht. Die Ausgestaltung solcher Systeme hat sich folglich an der DSGVO zu orientieren. Der Umstand, dass § 26 TTDSG selbst keine Vorgaben zur Wirksamkeit der Einwilligung macht, spricht dafür, dass der Bundesgesetzgeber seinen Kompetenzrahmen mit § 26 TTDSG nicht überschritten hat.

Weiterhin ist fraglich, inwieweit PIMS – und damit letztlich auch die Rechtsverordnung i. S. v. § 26 Abs. 2 TTDSG – den Anforderungen der DSGVO an die Einholung wirksamer Einwilligungen gerecht werden können. Eine Einwilligung muss nach Art. 4 Nr. 11 DSGVO für den konkreten Fall abgegeben werden. Der EuGH führt hierzu aus, dass sich eine Einwilligung gerade auf die betreffende und damit eine konkret stattfindende Datenverarbeitung beziehen muss.[48] Aus Erwägungsgrund 32 DSGVO ergibt sich weiter, dass Pauschaleinwilligungen nicht wirksam sind. PIMS verfolgen aber gerade den Zweck, dem Nutzer die Vielzahl an Einzelentscheidungen abzunehmen.[49] Das Konzept eines PIMS sieht vor, dass der Nutzer eine allgemeine Konfiguration seiner Privatsphäre-Einstellungen bereits im Vorfeld und damit unabhängig von der konkreten Nutzung eines Online-Angebotes vornimmt.[50] Bei konsequenter Betrachtung bedeutet dies, dass der Nutzer im Rahmen des PIMS eine abstrakt-generelle Entscheidung zu der Frage trifft, welche Technologien basierend auf seiner Entscheidung genutzt werden dürfen und wie konkret-individuell mit seinen Daten umgegangen werden darf.[51] Wenn man hierin nicht bereits grundsätzlich eine Abweichung von den Anforderungen der DSGVO an eine wirksame Einwilligung sehen will, muss man eine solche wohl spätestens dort bejahen, wo die Abläufe im Einzelfall von den im Rahmen der PIMS abgebildeten Regelfällen der Datenverarbeitung abweichen.[52] Soweit die Abweichung im Vorfeld nicht bedacht wurde, kann konsequenterweise schon gar keine Einwilligung für diesen konkreten Fall vorliegen und fehlt es folglich an einer wirksamen Einwilligung. Zum gleichen Schluss muss man wohl auch bezüglich der Information des Nutzers kommen.

Die technische Umsetzung von PIMS stellt sich angesichts der Vielzahl erforderlicher Verknüpfungen als komplex dar.[53] Insoweit ist zu vermuten, dass PIMS wohl am ehesten von den etablierten Tech-Giganten entwickelt werden. Dies birgt jedoch unter Umständen die Gefahr, dass die betreffenden Unternehmen bei der Umsetzung eines PIMS für sie selbst möglichst günstige Ausgestaltungen wählen, die Nutzer in ihren Entscheidungen interessenwidrig beeinflussen und die innerhalb des PIMS verarbeiteten Nutzerdaten für sich selbst nutzbar machen.[54] Diese Problematik soll durch § 26 Abs. 1 TTDSG adressiert werden, demzufolge Anbieter von PIMS bzw. PIMS selbst bestimmte Voraussetzungen wie nutzerfreundliche und wettbewerbskonforme Verfahren (Nr. 1), kein wirtschaftliches Eigeninteresse (Nr. 2) und ein Sicherheitskonzept (Nr. 4) sicherzustellen haben. Dass in Bezug auf diese Anforderungen die kompetenzrechtlichen Implikationen neben dem Datenschutzrecht stehender Rechtsmaterien, insbesondere des Wettbewerbs- und des Kartellrechts, bedacht worden wären, lässt sich den Gesetzgebungsmaterialien jedoch nicht entnehmen.

Die Europäische Kommission hat mit dem Data-Governance-Act (im Folgenden: DGA-E) einen Regelungsvorschlag u. a. in Bezug auf sog. Mittler für die gemeinsame Nutzung personenbezogener Daten, welche Einzelpersonen auch bei der Ausübung ihrer Betroffenenrechte unterstützen sollen, vorgestellt.[55] Auch wenn der eigentliche Zweck solcher Mittler nicht vollständig mit dem der PIMS vergleichbar ist, sollten die Bedingungen für die Erbringung von Mittlerdiensten als Orientierungsrahmen für PIMS dienen. Die in § 26 TTDSG statuierten Anforderungen sind mit denen des Art. 11 DGA-E auch grundsätzlich vergleichbar. Art. 11 DGA-E legt allerdings noch weitergehende Bedingungen fest. Neben einem fairen, transparenten und diskriminierungsfreien Zugang zu solchen Diensten (Nr. 3), haben die Anbieter von Mittlerdiensten etwa sicherzustellen, dass anfallende Metadaten ausschließlich für die Weiterentwicklung des angebotenen Dienstes genutzt werden (Nr. 2).

Grundsätzlich ist der Ansatz, die Abfrage von Einwilligungen mittels technischer Verfahren zur Einwilligungsverwaltung transparenter zu gestalten, begrüßenswert. Es stellt sich jedoch die Frage, ob die Einführung entsprechender Systeme tatsächlich zu einer differenzierten Auseinandersetzung mit der eigenen Entscheidungsbefugnis führt oder andererseits die unbedachte Abgabe von Einwilligungen durch diese noch erleichtert wird und ob insoweit die Regulierung der einwilligungsbedürftigen Verfahren nicht eigentlich der effektivere Ansatz wäre.[56]

V. Zusammenfassung

Es muss festgestellt werden, dass auch nach dem Inkrafttreten des TTDSG für die Rechtsanwender Unsicherheiten hinsichtlich der Unionsrechtskonformität nationaler Bestimmungen bestehen. Weiterhin dürfte zumindest unklar sein, ob Arbeitgeber, welche die Privatnutzung betrieblicher Kommunikationsmittel gestatten, als Anbieter von Telekommunikationsdiensten gelten. Soweit Arbeitgeber sich auch unter Berücksichtigung der dargestellten rechtlichen Implikationen dazu entscheiden sollten, die Nutzung betrieblicher Kommunikationsmittel zu privaten Zwecken zu erlauben, sollten sie dies nicht lediglich mittels (konkludenter) Duldung tun, sondern vielmehr eindeutige Regeln insoweit etablieren und etwaige einwilligungspflichtige Sachverhalte entsprechend legitimieren.

Im Hinblick auf PIMS stellt sich ganz prinzipiell die Frage, inwieweit Regelungen zur Einwilligungsverwaltung überhaupt von der Gesetzgebungskompetenz des Bundesgesetzgebers gedeckt sind. Gesteht man dem nationalen Gesetzgeber die Kompetenz zur grundsätzlichen Regulierung von PIMS zu, die unter dogmatischen, aber auch rein praktischen Gesichtspunkten angesichts der angestrebten Harmonisierung des Binnenmarktes fragwürdig ist, verbleibt außerdem die Frage, ob PIMS überhaupt den Anforderungen der DSGVO an die Einholung wirksamer Einwilligungen gerecht werden können. In Anbetracht dessen, dass eine die Anforderungen von § 26 TTDSG konkretisierende Rechtsverordnung noch nicht vorliegt, kommen

48 EuGH, 1. 10. 2019 – C-673/17, K&R 2019, 705 – Planet49.
49 *Assion*, Ausschussdrucksache 19(9)1039, S. 10.
50 *Engeler*, Ausschussdrucksache 19(9)1056, S. 3 f.
51 *Assion*, Ausschussdrucksache 19(9)1039, S. 11.
52 *Engeler*, Ausschussdrucksache 19(9)1056, S. 4.
53 *Assion*, Ausschussdrucksache 19(9)1039, S. 11.
54 Datenethikkommission der Bundesregierung, Gutachten, Oktober 2019, S. 133, abrufbar unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6.
55 Siehe hierzu Kapitel 3 DGA-E.
56 *Engeler*, Ausschussdrucksache 19(9)1056, S. 5.

diesen Fragestellungen allerdings derzeit noch keine praktischen Konsequenzen zu.

Auch angesichts des Umstandes, dass ein unter portugiesischer Ratspräsidentschaft entwickelter Entwurf einer E-Privacy-VO,[57] welche die E-Privacy-RL ablösen soll, derzeit den Gegenstand von Trilog-Verhandlungen bildet, scheint dem TTDSG lediglich eine verhältnismäßig kurze Lebensdauer bestimmt zu sein. Zum Thema Einwilligungsverwaltung sieht der derzeitige Entwurf jedenfalls ebenfalls vor, dass Einwilligungen auch über passende technische Einstellungen einer Software ausgedrückt werden können, Art. 4a VO-E.

57 2017/0003(COD).

Laura Schulte
Studium der Rechtswissenschaften an der Universität Bielefeld; Mitarbeiterin am Lehrstuhl von Prof. Dr. Gusy 2014 - 2019; Forschungsaufenthalt an der Queen Mary School of Law 2015; Promotion zum Dr. jur. 2017 („Vom quantitativen zum qualitativen Datenschutz"); Referendariat in Bielefeld und Bonn mit einer Station beim BSI; seit 2020 RAin in der Kanzlei BRANDI in Bielefeld.

Christina Prowald
ist wiss. Mitarbeiterin in der Kanzlei BRANDI Rechtsanwälte in Bielefeld im Bereich IT- und Datenschutzrecht. Ihr Studium absolvierte sie an der Universität Bielefeld. Während ihres Studiums war sie an einem zivilrechtlichen Lehrstuhl der Universität Bielefeld als studentische Hilfskraft tätig.

RA Dr. Ulrich Becker und RAin Sinje Maier*

Neuausrichtung der (europäischen) Marktüberwachung

Neue Product-Compliance-Pflichten

Kurz und Knapp

Am 16. 7. 2021 ist mit der Marktüberwachungsverordnung (EU 2019/1020) (MÜ-VO) eine der wesentlichsten Änderungen der vergangenen Jahre im Bereich des europäischen Produktsicherheitsrechts in Kraft getreten. Vor dem Hintergrund der Zielsetzung, den Online-Handel künftig besser kontrollieren zu können, sind insbesondere auch Fulfilment-Dienstleister und Betreiber von Online-Plattformen Adressaten neuer Pflichten. Der deutsche Gesetzgeber hat mit dem Marktüberwachungsgesetz (MüG) den Anwendungsbereich der MÜ-VO auf den nicht-harmonisierten Bereich erstreckt.

I. Hintergrund und Einordnung der MÜ-VO

Neu ist das Thema Marktüberwachung auf europäischer Ebene insbesondere vor dem Hintergrund der bis zum Inkrafttreten der MÜ-VO geltenden Marktüberwachungsverordnung (VO (EU) 765/2008) und dem Beschluss 768/2008/EG nicht. Vielmehr hatten die nationalen Marktüberwachungsbehörden bereits mit Geltung der vorstehenden Rechtsakte verschiedene Möglichkeiten, Sorge dafür zu tragen, dass nur sichere Produkte auf dem europäischen Markt bereitgestellt werden. Die eher auf die Harmonisierung von (formellen und materiellen) Produktanforderungen fokussierten Regelungen zur Produktsicherheit konnten zuletzt den Realitäten der Wirtschaft, insbesondere den komplexen Lieferketten des internationalen (Online-)Handels und den neuen Geschäftsmodellen, nicht mehr gerecht werden. Verfolgtes Ziel der MÜ-VO ist insofern das Schließen bestehender Lücken, insbesondere bezüglich auf dem EU-Markt agierender Akteure wie bspw. dem bis dato kaum greifbaren Fulfilment-Dienstleister oder den Verkaufsplattformen und Online-Händlern.[1] Zudem standen auch die Effizienz der an den EU-Außengrenzen durchgeführten Zollkontrollen in der Kritik.[2]

II. Anwendungsbereichsbezogene Aspekte

1. Sachlicher Anwendungsbereich

Die Geltung der MÜ-VO setzt zunächst die Eröffnung ihres sachlichen Anwendungsbereichs voraus, denn interessanterweise hat der Gesetzgeber die Geltung der MÜ-VO nicht für sämtliche Produkte vorgesehen. Das allerdings wäre im Sinne einer möglichst effizienten Marktüberwachung naheliegend gewesen. Vielmehr gilt die MÜ-VO für den europäisch-harmonisierten Produktbereich. Gemäß Art. 2 Abs. 1 findet sie auf all diejenigen Produkte Anwendung, die den im Anhang I der MÜ-VO genannten Harmonisierungsvorschriften unterfallen. Anhang I umfasst aktuell 70 EU-Rechtsakte; darunter Produktkategorien wie Maschinen, Verpackungen, Spielzeug, Druckgeräte, Bauprodukte, Elektrogeräte, Aufzüge, Funkanlagen oder persönliche Schutzausrüstung. Während das übrige europäische Produktsicherheitsrecht typischerweise auf konkret definierte Produkte bzw. Produktkategorien abstellt, bezieht die MÜ-VO mithin eine Vielzahl von EU-Rechtsakten vollumfänglich mit ein, gilt somit horizontal. Eine Unterscheidung zwischen Verbraucher- und Nicht-Verbraucherprodukten erfolgt nicht.

Interessant ist allerdings, dass die MÜ-VO einen differenzierten Anwendungsbereich beschreibt; denn wichtige Regelungen der MÜ-VO gelten wiederum nur für bestimmte Produkte (siehe hierzu unter III.).

* Mehr über die Autoren erfahren Sie am Ende des Beitrags.
1 Vgl. ErwG 13 zur MÜ-VO.
2 Vgl. ErwG 52 zur MÜ-VO.