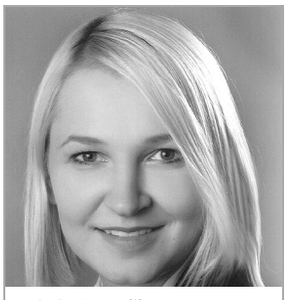
ROLF SCHWARTMANN / KRISTIN BENEDIKT / YVETTE REIF

Entwurf zum TTDSG: Für einen zeitgemäßen Online-Datenschutz?

Ein Zwischenruf

Mit der Schaffung eines Telekommunikations-Telemedien-Datenschutz-Gesetzes (TTDSG) soll ein Bündel an gesetzgeberischem Handlungsbedarf erledigt werden. Seit Inkrafttreten der DS-GVO besteht Rechtsunsicherheit bei der Anwendung des geltenden Rechts. Das komplexe Verhältnis zwischen europäischem Recht – der DS-GVO und ePrivacy-RL – und den weiterhin geltenden nationalen Vorschriften – dem TKG und dem TMG – soll auf nationaler Ebene mit dem TTDSG aufgelöst werden. Um für mehr Rechtsklarheit zu sorgen, beabsichtigt der Referentenentwurf die Vorschriften des Datenschutzes für Telemedien- und TK-Dienste, insbesondere das Fernmeldegeheimnis, in einem Gesetz neu zu regeln.

Prof. Dr. Rolf Schwartmann


Kristin Benedikt


Yvette Reif, LL.M.

Hinzu kommt, dass der deutsche Gesetzgeber verpflichtet ist, die Regelungen der Richtlinie über den europäischen Kodex für die elektronische Kommunikation (RL (EU) 2018/1972) bis zum 21.12.2020 umzusetzen. Der Kodex enthält eine Vielzahl von Regelungen, die den Wettbewerb im Bereich der elektronischen Kommunikation fördern sollen, und erweitert den sachlichen Anwendungsbereich, indem der Begriff der TK-Dienste an die technischen Entwicklungen angepasst wird. Unter TK-Dienste fallen Onlinedienste wie Internettelefonie, web-gestützte E-Mail-Dienste, Over-the-Top(OTT)-Dienste wie Messenger, aber auch Kommunikationseinrichtungen in Online-Spieleplattformen oder Online-Spieleforen sowie Chatfunktionen bei Onlinespielen (vgl. Art. 1 TKG, § 3 Nr. 24, 61 TKG-E). Die Umsetzung des Kodex soll durch das Telekommunikationsmodernisierungsgesetz (Entwurf eines Gesetzes zur Umsetzung der RL (EU) 2018/1972 des Europäischen Parlaments und des Rates v. 11.12.2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts) erfolgen.

I. Ausgewählte Regelungen des TTDSG-E

1. Anwendungsbereich des TTDSG

Das TTDSG soll neben der DS-GVO gelten und u.a. das Fernmeldegeheimnis, technische und organisatorische Anforderungen bei Telemedien und den Umgang mit Informationen auf Endeinrichtungen der Endnutzer regeln. Der sachliche Anwendungsbereich ist auf Grund von Verweisungen auf die Begriffsbestimmungen des TKG-E ebenfalls erweitert und umfasst insbesondere OTT-Kommunikationsdienste, Websites, Apps sowie den Bereich Internet of Things (IoT), §§ 1 f. TTDSG-E.

2. Einwilligung bei Endeinrichtungen

a) Anwendungsbereich und Inhalt der Regelung

§ 22 TTDSG-E enthält eine Regelung zum Einsatz von Cookies und vergleichbaren Technologien. Cookies sind kleine Textdateien, die der Webbrowser auf dem Computer speichert. Anhand von Cookies erkennt eine Website, wer sie gerade besucht, und kann dadurch Nutzerpräferenzen, wie z.B. Sprach- oder Bildschirmeinstellungen, oder Log-in-Informationen speichern, damit der Nutzer die Einstellungen nicht immer wieder neu vornehmen bzw. sich immer wieder neu anmelden muss. Beim Onlineshopping verhindern Cookies, dass sich mit jedem Aufruf einer neuen Unterseite im Rahmen des Webangebots der Warenkorb leert. Beim Online-Marketing ermöglicht der Einsatz von Cookies, die Nutzerinteressen auch Session-übergreifend zu ermitteln und so möglichst zielgenaue Onlinewerbung auszuspielen (zum Sinn von Cookies s.a. *Schwartmann/Benedikt/Reif*, RDV 2020, 231). Zunehmend werden allerdings alternative Trackingverfahren entwickelt, die eine Nachverfolgung des Nutzers auch ohne Cookies ermöglichen sollen („Cookieless Tracking") (*Schwartmann/Benedikt/Reif*, RDV 2020, 231 (234)). Die Regelung im TTDSG-E ist insofern technologieneutral. So würde z.B. auch das sog. Browser Fingerprinting der geplanten Regelung unterfallen.

Vom Anwendungsbereich des § 22 TTDSG-E erfasst sind auch die Vielzahl von Gegenständen im Internet der Dinge, die inzwischen – sei es direkt oder über einen WLAN-Router – an das öffentliche Kommunikationsnetz angeschlossen sind, etwa im Bereich von Smarthome-Anwendungen (z.B. Küchengeräte, Heizkörperthermostate, Alarmsysteme) (vgl. Begr. zu § 22 TTDSG-E).

Die geplante Regelung in § 22 TTDSG-E transferiert Art. 5 Abs. 3 ePrivacy-RL (RL 2002/58/EG) in der durch Art. 2 Nr. 5 RL 2009/136/EG geänderten Fassung in nationales Recht. Sie orientiert sich unmittelbar am Wortlaut der europäischen Vorgaben. § 22 TTDSG-E verlangt für die Speicherung von Informationen in Endeinrichtungen des Endnutzers bzw. den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, demgemäß regelmäßig eine Einwilligung. Ausnahmen vom Einwilligungserfordernis sollen nur gelten, wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder des Zugriffs auf diese Informationen die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist (§ 22 Abs. 2 TTDSG-E) bzw. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf diese Informationen unbedingt erforderlich ist, um einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen zu können (§ 22 Abs. 3 TTDSG-E).

b) Bewertung

Mit der geplanten Neuregelung gäbe es eine einheitliche Regelung für den Zugriff auf Endeinrichtungen, die unabhängig vom

Personenbezug in diesem Zusammenhang verarbeiteter Informationen greift. Letzteres entspricht den europäischen Vorgaben. Art. 5 Abs. 3 ePrivacy-RL soll den Nutzer vor jedem Eingriff in seine Privatsphäre schützen, unabhängig davon, ob dabei personenbezogene Daten oder andere Daten betroffen sind (*EuGH* MMR 2019, 732 m. Anm. *Moos/Rothkegel*, Rn. 68-71 – Planet49). Der Umweg über eine europarechtskonforme Interpretation von § 15 Abs. 3 TMG, den der *BGH* in seiner Entscheidung im Mai 2020 gehen musste (*BGH* MMR 2020, 609 m. Anm. *Gierschmann* – Cookie-Einwilligung II), entfiele. Dies ist auch deshalb begrüßenswert, weil der Weg über § 15 Abs. 3 TMG dogmatisch zweifelhaft erscheint (von einem „waghalsigen rechtsmethodischen Manöver" spricht *Spindler*, NJW 2020, 2513 (2517)), denn die Anwendbarkeit von Art. 5 Abs. 3 ePrivacy-RL auch auf nicht personenbezogene Daten lässt sich über die §§ 11 ff. TMG nicht abbilden (vgl. § 11 Abs. 1 TMG, wonach die Vorschriften dieses TMG-Abschnitts die „Erhebung und Verwendung personenbezogener Daten der Nutzer von Telemedien" regeln).

Wichtige praxisrelevante Fragen im Zusammenhang mit Cookies und vergleichbaren Verfahren bleiben allerdings ungelöst. Dies gilt etwa im Hinblick auf Cookies, die zur Websiteoptimierung (auch „Reichweitenmessung" oder „Analytics" – entgegen der Bezeichnung handelt es sich bei Google Analytics nicht um ein reines Analytics-Werkzeug) zum Einsatz kommen. An derartigen Verfahren besteht naturgemäß ein großes Interesse der Websitebetreiber. Diese in Abhängigkeit von einer Nutzereinwilligung zu stellen, ist problematisch, weil eine effektive Websiteoptimierung eine möglichst breite Datenbasis, eine wirksam erteilte Einwilligung aber deren Freiwilligkeit bedingt. Nach Ansicht der *Art. 29-Datenschutzgruppe* (Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, Stand: 7.6.2012, S. 11 f.) stellen First-Party-Analysecookies auch kaum ein Datenschutzrisiko dar, wenn sie nur für aggregierte Statistiken des Erstanbieters genutzt und von Websites verwendet werden, die in ihrer Datenschutzrichtlinie bereits unmissverständlich über die Cookies informieren und ausreichende Datenschutzgarantien bieten. Insofern sollte ein gesetzlicher Erlaubnistatbestand für Verfahren der Reichweitenmessung geschaffen werden. Auf Grund der engen Vorgaben der ePrivacy-RL, wonach Cookies „unbedingt erforderlich" für die Diensteerbringung sein müssen, was für Analysecookies zweifelhaft erscheint, würde allerdings über einer entsprechenden nationalen Regelung stets das Damoklesschwert der potenziellen Europarechtswidrigkeit hängen.

Ähnliches gilt für die im geleakten alten Referentenentwurf noch enthaltene Regelung zur Zulässigkeit sog. Cookie Walls, die u.a. im Bereich der Onlinepresse verbreitet sind. Denn auch hier stellt sich die Frage, ob eine nationale Regelung, welche die vertragliche Vereinbarung von nicht unbedingt erforderlichen Cookies gestattet (vgl. § 9 Abs. 2 Nr. 2 TTDSG-E des alten Referentenentwurfs), europarechtskonform wäre. Im Grunde droht jede nationale Abweichung vom Begriff der unbedingten Erforderlichkeit vor dem *EuGH* zu landen.

Insofern mag § 22 TTDSG-E zwar nicht der große Wurf sein, der alle rechtlichen Probleme im Zusammenhang mit Cookies und Cookie-ähnlichen Technologien auflöst. Angesichts der eingeschränkten nationalen Regelungskompetenz darf man diesen vom nationalen Gesetzgeber aber auch nicht erwarten. Im Sinne der bezweckten Rechtssicherheit erscheint es durchaus nachvollziehbar, dass der aktuelle Entwurf an dieser Stelle – anders als noch der geleakte Vorgängerentwurf – nicht mehr nach Regelungsspielräumen bzw. Konkretisierungsmöglichkeiten für den nationalen Gesetzgeber sucht, sondern sich eng an der ePrivacy-RL orientiert und die Lösung zentraler Themen damit auf die europäische Ebene verlagert. Leider hakt der europäische Einigungsprozess aber weiterhin und auch die deutsche Ratspräsidentschaft konnte zuletzt keine Verständigung herbeiführen. Eine umfassende Lösung für den Einsatz von Cookies und vergleichbaren Techniken ist damit weiterhin nicht in Sicht.

Geboten ist eine deutlichere Klarstellung des Verhältnisses von § 22 TTDSG-E zum Datenschutzrecht. Klar erscheint, dass § 22 TTDSG-E unabhängig davon gelten soll, ob mit dem Cookie Einsatz eine Verarbeitung personenbezogener Daten einhergeht. Für den Fall, dass Letzteres der Fall ist, stellt sich allerdings die Frage, ob § 22 TTDSG-E Rechtsgrundlage auch für die mit dem Setzen bzw. Auslesens des Cookies verbundene personenbezogene Datenverarbeitung ist. Die Gesetzesbegründung geht auf das Verhältnis zwar ein, die betreffende Passage ist jedoch nicht eindeutig.

3. Technische und organisatorische Regelungen

Nach dem Referentenentwurf sollen Anbieter von Telemedien die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym ermöglichen, soweit dies technisch möglich und zumutbar ist. Auch eine Weiterleitung zu einem anderen Diensteanbieter ist dem Nutzer anzuzeigen, vgl. § 19 TTDSG-E.

Diese Regelungen greifen die bisher geltenden Vorschriften des § 13 Abs. 5 und 6 TMG auf. Es überrascht, dass diese antiquierten Vorschriften des TMG in die Gesetzesnovelle aufgenommen werden sollen. Die Anforderungen gelten zu Recht als technisch und rechtlich überholt (*Schmitz*, in: *Spindler/Schmitz*, TMG, Komm., 2. Aufl. 2018, § 13 Rn. 62) und in der Praxis nahezu nicht umsetzbar. Eine anonyme Nutzung ist bereits technisch unmöglich, da bei der elektronischen Kommunikation eine Vielzahl von (Geräte)-Kennungen verwendet wird, um die Diensterbringung zu ermöglichen. Auch eine pseudonyme Nutzung dürfte in vielen Fällen weder technisch möglich noch zumutbar sein. Vor allem bei Social-Media-Plattformen oder Messengern ist es unabdingbar, dass die Identität der Nutzer bekannt ist. Ob eine pseudonyme Nutzung zumutbar ist, bestimmt sich in erster Linie nach dem Geschäftsmodell des Anbieters von Telemedien (*Roßnagel*, Beck'scher Komm. Telemediendienste, 1. Aufl., TMG § 13 Rn. 130). Fordert ein Anbieter die Anmeldung seiner Nutzer unter Klarnamen und kann er dies im Einzelfall plausibel begründen, so ist er von der Pflicht, eine anonyme oder pseudonyme Nutzung zu ermöglichen, befreit. Die Regelungen des § 19 Abs. 2 TTDSG-E dürften daher in der Praxis leerlaufen (vgl. *LG Frankfurt/M.* U. v. 3.9.2020 – 2-03 O 282/19 = zur Rechtmäßigkeit einer Klarnamenspflicht in einem sozialen Netzwerk).

Die Pflicht, eine anonyme oder pseudonyme Nutzung zu ermöglichen, konterkariert zudem das gesetzgeberische Ziel, Hasskriminalität im Internet zu bekämpfen. Volksverhetzung, Beleidigungen und Bedrohungen bei sozialen Netzwerken, Messengern und sonstigen Plattformen haben Hochkonjunktur. Für viele Täter erscheint das Internet ein rechtsfreier Raum. Eine strafrechtliche Verfolgung scheitert häufig daran, dass Täter unter Pseudonymen handeln und eine Identifizierung erschwert ist. Aus diesem Grund werden gesetzliche Regelungen zur eindeutigen Identifizierbarkeit von Tätern im Zusammenhang mit Hasskriminalität im Internet diskutiert (Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 212. Sitzung der *Ständigen Konferenz der Innenminister und -senatoren der Länder* v. 17. bis 19.6.2020 in Erfurt (TH), TOP 24).

Auch die Pflicht, eine Weiterleitung an einen anderen Diensteanbieter dem Nutzer anzuzeigen, dürfte in der Praxis ihren Zweck verfehlen. Die Vorschrift ist auf Fälle anwendbar, in denen ein Website Besucher einen Link auf einer Website anklickt und hierdurch auf eine weitere Website weitergeleitet wird. Diese Form der klassischen Weiterleitung ist jedoch ein Auslaufmodell. Der

Websitebetreiber möchte in aller Regel verhindern, dass der Nutzer sein Onlineangebot verlässt, indem er auf einen Link klickt. Aus diesem Grund werden unter anderem Drittinhalte auf Websites eingebunden. Der Websitebesucher kann Werbebanner, Videos oder Kartendienste nutzen, ohne die Website verlassen zu müssen. Umstritten ist, ob bei der Einbindung von Drittinhalten die Pflicht zur Anzeige der Weiterleitung gilt. Da der Nutzer den genutzten Onlinedienst nicht verlässt, findet technisch betrachtet keine Weiterleitung statt. Eine Anzeigepflicht gilt in diesen Fällen nicht (*Roßnagel*, a.a.O., Rn. 118), sodass der Mehrwert einer solchen Regelung äußerst fraglich ist.

4. Zuständige Aufsichtsbehörde und Sanktionen

Bisher war die Zuständigkeit klar geregelt. Der oder die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) war für den Vollzug des TKG zuständig; die Datenschutzaufsichtsbehörden der Länder hingegen für den Vollzug des TMG. Dies soll sich künftig ändern. Nach dem Referentenentwurf ist beabsichtigt, dem oder der *BfDI* die Zuständigkeit zu übertragen, soweit Anbieter von TK-Diensten oder öffentliche Stellen des Bundes die Regelung des § 22 TTDSG-E – Einwilligung bei Endeinrichtungen – beachten müssen. Durch diese Zuständigkeitserweiterung soll sichergestellt werden, dass der Zugriff auf Endeinrichtungen und die Verarbeitung von personenbezogenen Daten nur von einer Aufsichtsbehörde kontrolliert wird.

Diese (teilweise) Zentralisierung des Vollzugs der datenschutzrechtlichen Regelungen des TTDSG scheint verfassungsrechtlich unbedenklich, da für Angelegenheiten, für die dem Bund die Gesetzgebung zusteht, der Vollzug durch Bundesbehörden möglich ist, vgl. Art. 87 Abs. 3, Art. 73 Abs. 1 Nr. 7, Art. 74 Abs. 1 Nr. 11 GG.

Überraschend ist, dass der Referentenentwurf einen deutlich milderen Bußgeldrahmen bei einem Verstoß vorsieht als die DS-GVO. War in dem ersten Entwurf zum TTDSG noch eine Anlehnung an die Bußgeldvorschriften der DS-GVO beabsichtigt, soll künftig ein Verstoß gegen § 22 TTDSG-E „nur" noch mit einem Bußgeld von bis zu 300.000,– EUR geahndet werden, vgl. § 24 Abs. 1 Nr. 13, Abs. 2 TTDSG-E.

5. Verzicht auf Regelung zu Personal Information Management Services (PIMS)

Im aktuellen Entwurf ist die im geleakten Referentenentwurf aus Juli 2020 noch enthaltene Regelung zu Diensten zur Verwaltung persönlicher Informationen (§ 3 TTDSG-E alt) nicht mehr vorgesehen. Diese nicht wieder aufzunehmen, wäre ein Fehler. Die Norm ging auf eine Empfehlung der *Datenethikkommission (DEK)* zurück, die Datentreuhandsystemen ein großes Potenzial attestiert (Gutachten der *Datenethikkommission* (2019), Handlungsempfehlung 21).

Die Idee ist, dass Nutzer auf Dashboards Datenschutzeinstellungen vornehmen, die von den Diensteanbietern übernommen werden müssen. Um die Vielzahl der Angebote mit den Anfragen der Nutzer zu verknüpfen, bedarf es eines zwischengeschalteten Dienstes, der die Privacy-Einstellungen der Nutzer treuhänderisch verwaltet, ohne an der Nutzung der Daten zu verdienen. Da der Login zu den Angeboten im Netz dann nicht mehr über Facebook, Google, Amazon und zunehmend Apple erfolgt, sondern über einen europäischen Treuhänder, der sich offenen Standards unterwirft und Daten nach der Vorgabe des Schrems-II-Urteils des *EuGH* verarbeitet und speichert, könnten mit diesem Mittel Nutzerinteressen nach europäischen Datenschutzstandards durchgesetzt werden. Die nicht europäischen Diensteanbieter, die per Login Nutzerdaten erhalten und auswerten, wären nur dann berechtigt in Europa ihre Dienste anzubieten, wenn sie sich den europäischen Standards für Datentreuhänder unterwerfen. Dieser Ansatz ist vor dem Hintergrund sehr bedeutsam, dass der datengetriebene Nutzerkontakt nach der Praxis der großen Browseranbieter bereits heute über die Nutzer-ID erfolgt und nicht mehr durch Cookies oder alternative Methoden wie Fingerprinting.

Die Regelung in § 3 TTDSG-E alt war insofern grundsätzlich zu begrüßen. Sie war allerdings insofern missverständlich, als sie nicht eindeutig formulierte, dass entsprechende Angebote nur von akkreditierten Datentreuhändern erbracht werden dürfen. Nur im Falle eines solchen Verständnisses würde aber ein Anreiz zur Akkreditierung bestehen.

Ein Problem der Norm bestand auch darin, dass sie keine Vorkehrungen dafür traf, dass der Anbieter eines Browsers auch an die Einstellungen der Datenschutzvorgaben durch den Nutzer – sei es eine Einwilligung zum Tracking oder die Ablehnung – gebunden ist und die Einstellungen nicht beim Ausspielen seiner Angebote ignoriert. Man hätte sie um eine Regelung ergänzen müssen, die Anbieter in Verkehr gebrachter Software zum Betrieb von Netzkommunikation verpflichtet, nur anerkannten Diensten zur Verwaltung persönlicher Informationen eine Schnittstelle zur Übermittlung der Einwilligungsentscheidung des Nutzers zu bieten. Im Falle der Einwilligung des Nutzers müssten Speicherung und Zugriff auf Informationen auf dem Endgerät technisch ermöglicht werden.

Der Weg über eine verpflichtende Schnittstelle hätte der Empfehlung der *DEK* entsprochen, die in ihrem Abschlussgutachten ausführt: „PMT/PIMS können nur dann verlässlich arbeiten, wenn eine Kooperation mit allen betroffenen Verantwortlichen sichergestellt ist. Dabei ist eine hinreichende Breitenwirkung nur durch eine – unter sachgerechten Bedingungen stehende – rechtliche Verpflichtung für Verantwortliche im Sinne der DS-GVO zu erreichen, die Kontrolle des Zugangs zu personenbezogenen Daten durch PMT/PIMS zu ermöglichen und beispielsweise sicherzustellen, dass jede datenschutzrelevante Information das PMT/PIMS erreicht und das PMT/PIMS in Bezug auf alle personenbezogenen Daten die Interessen der betroffenen Person wahrnehmen kann."

Sinnvoll wäre zudem eine Klarstellung, wonach PIMS-Anbieter zwar nicht an der Nutzung der verwalteten Daten verdienen, für ihre Dienste aber durchaus Entgelte erheben dürfen.

Das Argument, das ursprüngliche Vorhaben mit Blick auf den auf europäischer Ebene geplanten Data Governance Act zurückzustellen, überzeugt nicht. Das Stocken des ePrivacy-Prozesses zeigt, wie wichtig Impulse aus den Mitgliedstaaten für die europäische Regulierung sind. Hier sollte Deutschland seine Rolle als Impulsgeber wahrnehmen (zur rechtlichen Zulässigkeit der verpflichtenden Einführung eines EU-Single-Sign-On: *Hofmann/Schwartmann/Weiß*, Kurzgutachten im Auftrag der European netID Foundation (netID), Januar 2021, abrufbar unter https://enid.foundation/wp-content/uploads/2021/01/Hofmann_Schwartmann_Weiss_Kurzgutachten_SSO_netID_20210119.pdf). Allerdings macht am Ende nur eine einheitliche europäische PIMS-Regelung Sinn. Deshalb sollte der deutsche Gesetzgeber sich im TTDSG am Entwurf des Art. 11 *Data Governance Act* v. 25.11.2020 orientieren und keine geringeren Anforderungen an PIMS formulieren.

II. Fazit

■ § 22 TTDSG-E sieht eine einheitliche Regelung für den Zugriff auf Endeinrichtungen vor, die unabhängig vom Personenbezug in diesem Zusammenhang verarbeiteter Informationen greift und insofern den europäischen Vorgaben entspricht. Ob § 22 TTDSG-E zugleich datenschutzrechtliche Rechtsgrundlage für die mit dem Setzen bzw. Auslesen des Cookies verbundene personenbezogene Datenverarbeitung ist, erscheint nicht eindeutig. Das Verhältnis zum Datenschutzrecht sollte konkretisiert werden.

- First-Party-Analysecookies und vergleichbare Techniken, um die Reichweite von Onlinediensten zu messen und verbessern, sollten auch ohne Nutzereinwilligung möglich sein. Für diese Position, die auch der Auffassung der Art.-29-Datenschutzgruppe entspricht (I.2.b), sollte sich die Bundesregierung i.R.d. Verhandlungen zur ePrivacyVO einsetzen.
- I.R.d. § 22 TTDSG-E sollte dem Umstand Rechnung getragen werden, dass häufig eine Vielzahl von Akteuren am Zugriff auf Endeinrichtungen und an der (anschließenden) Verarbeitung personenbezogener Daten beteiligt ist. Unklar ist bisher, wer das Einwilligungserfordernis des § 22 TTDSG-E in der Praxis umsetzen muss. Dies gilt u.a. bei Website-Betreibern, die selbst weder auf Informationen von Endeinrichtungen zugreifen noch Daten verarbeiten, sondern dies lediglich durch Einbindung auf der Website ermöglichen (z.B. bei Reichweitenanalyse).
- Mittels zertifizierter Datentreuhänder könnten Nutzerinteressen nach europäischen Datenschutzstandards wirksam durchgesetzt werden. Der Gesetzentwurf sollte daher – unter Berücksichtigung der im Artikel beschriebenen Rahmenbedingungen – wieder um eine Regelung zu Personal Information Management Services (PIMS) ergänzt werden.

Prof. Dr. Rolf Schwartmann
ist Leiter der Kölner Forschungsstelle für Medienrecht, Technische Hochschule Köln, sowie Vorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) in Bonn und Mitglied der Datenethikkommission. Zugleich ist er Mitglied im Stiftungsrat der European netID Foundation.

Kristin Benedikt
ist Richterin am Verwaltungsgericht Regensburg.

RAin Yvette Reif, LL.M.,
ist stellvertretende Geschäftsführerin der GDD.