Kapellmann
Rechtsanwälte

Das neue TTDSG - Was Anbieter von Webseiten, Apps und "smarten" Produkten jetzt beachten müssen

03. Dezember 2021

Am 01.12.2021 ist das neue Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG) in Kraft getreten. Mit dem TTDSG sind nun die datenschutzrechtlichen Vorschriften des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) in einem Gesetz zusammengefasst und neugeregelt worden. Von den neuen Vorgaben sind nicht nur sämtliche **Webseiten- und App-Betreiber** betroffen, sondern vielmehr auch Anbieter von „smarten" Produkten etwa aus dem **Smart Home-Bereich** oder von **sonstigen IoT-Lösungen**. Das TTDSG bringt zudem endlich mehr Rechtssicherheit in Bezug auf die im Online-Marketing lange Zeit umstrittene Frage, unter welchen Voraussetzungen der Einsatz von Cookies und ähnlichen Technologien in Deutschland datenschutzrechtlich zulässig ist. Andere zentrale Fragen bleiben gleichwohl ungeklärt, so dass die weiteren Entwicklungen in der Rechtsprechung abzuwarten sind.

Hintergrund

Insbesondere die Datenschutzaufsichtsbehörden hatten bereits seit längerer Zeit eine Anpassung der Datenschutzbestimmungen des TKG und TMG an die neuen Vorgaben der Europäischen Datenschutz-Grundverordnung (DS-GVO) gefordert und hierbei zugleich die unzureichende Umsetzung der sog. **ePrivacy-Richtlinie** (auch: „Cookie-Richtlinie") in das deutsche Recht, insb. in TKG und TMG bemängelt. Die DS-GVO ist seit Mai 2018 das primäre Regelwerk für den Datenschutz in der EU. Ergänzt wird die DS-GVO durch die bereits seit 2002 geltende ePrivacy-Richtlinie, die Mindestvorgaben für den Datenschutz konkret im Bereich der elektronischen Kommunikation vorsieht und mitunter auch die Frage regelt, unter welchen Voraussetzungen Diensteanbieter – etwa mittels Cookies, Pixel oder Fingerprints – Informationen auf Endgeräten von Nutzern speichern bzw. auf Informationen, die im Endgerät gespeichert sind, zugreifen dürfen.

Seit Geltung der DS-GVO sorgte das **Nebeneinander von DS-GVO, ePrivacy-Richtlinie, TMG und TKG** zu weiteren Unklarheiten sowohl bei den Nutzern von Telemedien und elektronischen Kommunikationsdiensten als auch bei den Anbietern solcher Dienste. Der Gesetzgeber sah gleichwohl zunächst von einer Neuregelung der Datenschutzbestimmungen im Telekommunikations- und Telemedienbereich ab, dies insbesondere deshalb, weil es auf europäischer Ebene Bestrebungen gab und nach wie vor gibt, die ePrivacy-Richtlinie umfassend durch eine unmittelbar geltende Europäische Verordnung abzulösen und zu novellieren. Ursprünglich war dabei geplant, dass die ePrivacy-Verordnung zeitgleich mit der DS-GVO in Kraft tritt. Das Vorhaben ist allerdings gescheitert. Derzeit ist immer noch nicht absehbar, wann eine Einigung erzielt und die ePrivacy-Verordnung verabschiedet wird.

Vor dem Hintergrund dieser Entwicklungen, der anhaltenden Kritik in Bezug auf die unklare Rechtslage und der sog. Planet49-Entscheidungen von EuGH und BGH (siehe dazu unten) sah sich der deutsche Gesetzgeber gezwungen, zumindest „*übergangsweise*" bis zur Geltung der ePrivacy-Verordnung mit dem TTDSG **mehr Rechtsklarheit zum Datenschutz in der digitalen Welt** zu schaffen.

Wer ist von den neuen TTDSG-Vorschriften betroffen?

Das TTDSG regelt primär den Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien, § 1 Abs. 1 Nr. 2 TTDSG. Von den Regelungen des TTDSG sind daher sowohl Anbieter von Telemedien als auch Telekommunikationsanbieter betroffen.

Anbieter von Telemedien ist nach § 2 Abs. 2 Nr. 1 TTDSG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt". Der Begriff der Telemedien ist dabei sehr weit gefasst. Nach § 1 Abs. 1 S. 1 TMG sind dies alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind. Unter den Telemedienbegriff fallen somit alle typischen Angebote im Online-Bereich wie Internet-Suchmaschinen, Online-Shops, Werbemails, Video-on-Demand-Dienste oder auch nur rein informatorische Webseiten oder Apps. Aufgrund dieses weiten Verständnisses sind sämtliche Unternehmen und öffentliche Stellen, die eine **eigene Webseite betreiben oder Apps anbieten**, von der Gesetzesänderung betroffen.

Darüber hinaus sollten aber auch Anbieter von Smart Home-Geräten, die an das öffentliche Kommunikationsnetz angebunden sind, wie etwa Smart-TVs, intelligente Küchenhelfer, Hausnotrufsysteme oder Heizkörperthermostate, die neuen Bestimmungen des TTDSG im Blick haben. Gleiches gilt für Lösungen im Bereich des vernetzten und automatisierten Fahrens. Für sie wird insbesondere der in den letzten Monaten in der Öffentlichkeit viel diskutierte § 25 TTDSG relevant, der ein grundsätzliches Einwilligungserfordernis für den Einsatz von nicht unbedingt notwendigen Cookies und ähnlichen Technologien vorsieht (siehe dazu unten). Der Anwendungsbereich dieser Norm ist bewusst technikneutral und sehr weit formuliert. Erfasst ist letztlich jede Speicherung von Informationen in einer Endeinrichtung des Nutzers bzw. jeder Zugriff auf die in einer Endeinrichtung gespeicherten Informationen, wobei „Endeinrichtung" jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten ist (§ 2 Abs. 2 Nr. 6 TTDSG). Nach der Gesetzesbegründung sind damit nicht nur Telefonie oder Internetkommunikation erfasst, sondern alle **Smart-Geräte und Produkte im „Internet der Dinge" (IoT)**, die an das öffentliche Kommunikationsnetz angeschlossen sind.

Der Begriff des **Telekommunikationsanbieters** bestimmt sich nach dem ebenfalls novellierten TKG (§ 2 Abs. 1 TTDSG). Dieses erfasst nicht nur sog. nummerngebundenen interpersonellen Telekommunikationsdienste, sondern nunmehr auch sog. nummernunabhängige interpersonelle Kommunikationsdienste (§ 3 TKG-neu). Mithin richten sich die telekommunikationsrechtlichen Vorschriften fortan auch an sog. Over-the-top-Kommunikationsdienste (OTT), etwa webgestützte E-Mail-Dienste oder Messenger wie WhatsApp.

Telekommunikationsdatenschutz – Alter Wein in neuen Schläuchen?

Das TTDSG enthält in Teil 2 (§§ 3 bis 18) die Bestimmungen zum Datenschutz in der Telekommunikation. Hier finden sich Regelungen zum Fernmeldegeheimnis, zur Verarbeitung von Verkehrs- und Standortdaten, zur Rufnummernanzeige und -unterdrückung, zu Endnutzerverzeichnissen sowie zur Bereitstellung von

Endnutzerdaten.

Inhaltlich finden sich in diesem Teil **keine grundlegenden Neuerungen**. Im Kern überführt der Gesetzgeber die bislang in §§ 88 ff. TKG enthaltenen Regelungen nun in das TTDSG. Neu ist lediglich, dass sich die telekommunikationsrechtlichen Datenschutzvorschriften mit Inkrafttreten des TTDSG auch an OTT-Kommunikationsdienste richten. Damit sind die strengen telekommunikationsrechtlichen Vorgaben nun von einem erweiterten Adressatenkreis wie E-Mail- oder Messenger-Diensteanbieter zu beachten.

Neue Regelungen für Cookies und Co.?

Insbesondere im Zusammenhang mit dem Einsatz von Cookies wurde in Deutschland jahrelang die Umsetzung von Art. 5 Abs. 3 ePrivacy-Richtlinie durch die Vorschriften in §§ 11 ff. TMG kontrovers diskutiert.

Art. 5 Abs. 3 ePrivacy-Richtlinie sieht für die Speicherung von und den Zugriff auf Informationen auf Endgeräten als Grundsatz ein **Einwilligungserfordernis** vor. Da EU-Richtlinien im Gegensatz zu EU-Verordnungen in den Mitgliedsstaaten nicht unmittelbar anwendbar sind, hätte der deutsche Gesetzgeber das Erfordernis der expliziten Einwilligung eigentlich in nationales Recht umsetzen müssen. Hier fand sich bis dato in § 15 Abs. 3 Satz 1 TMG jedoch lediglich eine „Widerspruchslösung" – eine explizite Einwilligung forderte der Wortlaut der Norm gerade nicht. Dies war und ist nach wie vor der Grund dafür, dass auf Webseiten häufig keine Einwilligung der Nutzer für Trackingtechnologien wie Google Analytics über eine sog. Consent Management Platform („Cookie-Banner") eingeholt, sondern unter Verweis auf § 15 Abs. 3 Satz 1 TMG lediglich ein entsprechender pauschaler Hinweis auf das Widerspruchsrecht eingeblendet wird (z.B. „*Diese Website verwendet Cookies und andere Technologien, um die Nutzung der Website zu analysieren. Sie können dem Setzen von Cookies jederzeit widersprechen. Weitere Informationen finden Sie in der Datenschutzerklärung.*"). Die überwiegende Rechtspraxis und die Datenschutzbehörden hielten dieses Vorgehen mit Blick auf das in Art. 5 Abs. 3 ePrivacy-Richtlinie klar statuierte Einwilligungserfordernis indes nicht für rechtskonform und sahen in § 15 Abs. 3 Satz 1 TMG eine unzureichende Umsetzung der europäischen Vorgaben.

Dieser jahrelange Streit erfuhr in der **Rechtssache *„Planet 49"*** seinen Höhepunkt. Mit der sog. *Planet 49*-Entscheidung stellte der EuGH klar, dass nach den Vorgaben der ePrivacy-Richtlinie technisch nicht notwendige Cookies, insbesondere Trackingtechnologien, einer wirksamen Einwilligung bedürfen (Urt. v. 01.10.2019, Az. C-673/17). Damit erteilte er der Widerspruchslösung ebenso eine klare Absage wie vorangekreuzten Einwilligung-Kästchen (sog. Opt-out). Der BGH sorgte dann kurz darauf mit der daran anknüpfenden *Cookie-Einwilligung-II*-Entscheidung für Aufruhr, indem er § 15 Abs. 3 Satz 1 TMG entgegen des eigentlich klaren Wortlauts in sehr „kreativer" Weise richtlinienkonform auslegte (Urt. v. 28.05.2020, Az. I ZR 7/16). Im Ergebnis forderte der BGH für die Speicherung nicht notwendiger Cookies auf dem Endgerät des Nutzers ebenfalls die Einholung einer expliziten Einwilligung, obgleich der Wortlaut des § 15 Abs. 3 Satz 1 TMG dies nicht ansatzweise hergab.

§ 25 TTDSG setzt dieser äußerst fragwürdigen Auslegung über die Wortlautgrenze hinaus ein Ende und bringt endgültig Rechtssicherheit. Die Norm fordert nun **explizit eine ausdrückliche Einwilligung** für das Setzen von Cookies, Web-Beacons, Pixel, Fingerprints und anderen Technologien, die Informationen auf dem Endgerät des Nutzers speichern oder auf solche Informationen zugreifen. Zu beachten ist dabei, dass § 25 TTDSG sich nicht nur auf personenbezogene Daten, sondern auf sämtliche „Informationen" bezieht. Ausnahmen vom Einwilligungserfordernis gelten nur in den Fällen des § 25 Abs. 2 TTDSG. Danach dürfen beispielsweise unbedingt erforderliche Cookies auf Webseiten weiterhin ohne Einwilligung der Nutzer gesetzt werden. Dies betrifft insbesondere Cookies, die für den funktionsgerechten Betrieb einer Webseite oder App oder zur Gewährleistung der technischen Webseite notwendig sind (z.B. zur Speicherung von Spracheinstellungen, von Nutzereingaben oder ausgewählten Produkten im Warenkorb). Letztlich erfordert die Bewertung, was als unbedingt erforderlich anzusehen ist und was nicht, einer Einzelbetrachtung unter Berücksichtigung des jeweiligen Dienstes.

§ 26 TTDSG schafft zudem den rechtlichen Rahmen für einheitliche Verfahren und technische Anwendungen zur zentralen Einwilligungsverwaltung. Mit der Einführung sog. Personal-Information-Management-Systeme (PIMS) will der Gesetzgeber dem Bedürfnis der Nutzer Rechnung tragen, die Cookie-Einstellungen zentral für verschiedene Webseiten auf allen Endgeräten zu steuern. Die „lästigen" Cookie-Banner wären dann entbehrlich. Derartige Dienste zur Einwilligungsverwaltung müssen allerdings strengen Anforderungen genügen und von einer unabhängigen Stelle anerkannt werden. Die Einzelheiten hierzu sind durch die Bundesregierung in einer Rechtsverordnung zu regeln. Bis zum Erlass der Rechtsverordnung und Einführung anerkannter PIMS am Markt werden sich Cookie-Banner noch großer (Un-)Beliebtheit erfreuen.

Alle Unklarheiten durch das TTDSG beseitigt?

Mit dem TTDSG ist es dem Gesetzgeber zudem nicht gelungen, alle Unklarheiten zu beseitigen. Das betrifft insbesondere die Anforderungen, die an eine wirksame

Einwilligung und an die Ausgestaltung von Cookie-Bannern zu stellen sind.

Für die Voraussetzungen einer wirksamen Einwilligung verweist § 25 Abs. 1 TTDSG zwar nun ausdrücklich auf Art. 4 Nr. 11, Art. 7 DS-GVO. Die Einwilligung muss also „ausdrücklich", „in informierter Weise", „für einen bestimmten Fall" und „freiwillig" erteilt werden und jederzeit widerrufbar sein. Was dies jedoch für die genaue **optische und inhaltliche Ausgestaltung des Cookie-Banners** und die darüber bereitzustellenden Informationen bedeutet, ist im Einzelnen nicht geregelt. Am Markt gibt es dabei mittlerweile zahlreiche Anbieter, die Einwilligungslösungen in ganz unterschiedlicher Ausführung anbieten. Häufig wird mit der „DS-GVO-Konformität" geworben. Dabei ist jedoch zu beachten, dass oftmals umfangreiche Konfigurations- und Gestaltungsmöglichkeiten existieren (z.B. Mehrstufigkeit und Differenzierungsmöglichkeit, Auswahl an Texten), die der Webseitenbetreiber letztlich eigenverantwortlich einrichten muss. Auch wird seitens des Online-Marketings gerne auf gestalterische „Tricks" zurückgegriffen, um die Einwilligungsrate erhöhen (z.B. durch Nudging und Dark Patterns). Bei dem Einsatz von Technologien, die mit **Datenübermittlungen in Drittländer (z.B. USA)** verbunden sind, sind zudem besondere Hinweispflichten zu beachten. Es bedarf daher einer genauen Prüfung, inwieweit Cookie-Banner sich in ihrer Ausgestaltung im zulässigen Rahmen bewegen und die Einholung einer wirksamen Cookie-Einwilligung tatsächlich gewährleisten. Tendenziell gilt ein strenger Maßstab, wie nicht zuletzt der BGH in seiner *Cookie-Einwilligung II*-Entscheidung deutlich gemacht hat.

Unklar ist weiterhin, inwieweit Cookies, die zwar nicht zu Analyse- und Werbezwecken dienen, aber zur Optimierung des Online-Angebots eingesetzt werden und damit jedenfalls in technischer Hinsicht nicht „unbedingt erforderlich" sind, einer Einwilligung bedürfen. Insoweit bleibt die weitere Rechtsentwicklung abzuwarten

Nach wie vor ungeklärt bleibt schließlich die höchst umstrittene Frage, inwieweit **Arbeitgeber**, die ihren Mitarbeitern die **private Nutzung der betrieblichen Kommunikationseinrichtungen** (insb. E-Mail und Internet) gestatten, als Diensteanbieter einzuordnen sind mit der Folge, dass sie das Fernmeldegeheimnis zu wahren haben und weder den Inhalt der Telekommunikation und Internetnutzung noch ihre näheren Umstände zur Kenntnis nehmen dürfen. Die überwiegende Rechtsprechung lehnt dies richtigerweise ab, eine höchstrichterliche Entscheidung steht gleichwohl noch aus.

Bedeutung für die Praxis?

Wenngleich das TTDSG keine tiefgreifenden Änderungen gegenüber der bisherigen Rechtslage unter Beachtung der *Cookie-Einwilligung II*-Entscheidung des BGH bringt, fällt in der Praxis immer wieder auf, dass die neuen Maßstäbe nicht hinreichend umgesetzt und Cookie-Banner nicht gesetzeskonform ausgestaltet sind.

Unternehmen und öffentliche Stellen sind daher gut beraten, anlässlich der gesetzlichen Neuregelung eine Überprüfung der auf Webseiten und in Apps eingesetzten Cookies und vergleichbaren Technologien vorzunehmen und insbesondere die Ausgestaltung der **Consent Management-Tools („Cookie-Banner")** einer kritischen Überprüfung zu unterziehen. Dabei sollte auch geprüft werden, welche der eingesetzten Technologien „unbedingt erforderlich" und welche einwilligungsbedürftig sind. Ebenso sind die im Cookie-Banner und in der **Datenschutzerklärung** bereitgestellten Informationen auf Richtigkeit, Verständlichkeit und Vollständigkeit zu überprüfen. Anbieter von „smarten" Produkten sollten zudem prüfen, inwieweit sie in den Anwendungsbereich des TTDSG fallen.

Verstöße gegen diese Vorgaben können unter dem TTDSG mit einer **Geldbuße von bis zu 300.000 € sanktioniert** werden. Soweit zugleich ein Verstoß gegen die Vorgaben der DS-GVO vorliegt, drohen sogar höhere Geldbußen. Gegen eine spanische Fluggesellschaft wurde etwa wegen datenschutzwidriger Ausgestaltung eines Cookie-Banners eine Bußgeld in Höhe von 30.000 € verhängt, gegen Google und Amazon wurden sogar Bußgelder in Höhe von 100 bzw. 35 Mio. € verhängt.

In diesem Kontext ist auch zu beachten, dass der Einsatz von Drittanbieter-Cookies und Tracking-Tools häufig mit **Datentransfers in Drittländer**, insbesondere in die USA verbunden ist. In diesem Fall ist zu prüfen, auf welcher Rechtsgrundlage die Übermittlung erfolgt. Der in Datenschutzerklärungen häufig noch anzutreffende Verweis auf das sog. EU US Privacy Shield ist seit der sog. Schrems II-Entscheidung des EuGH nicht mehr wirksam. Die deutschen Datenschutzaufsichtsbehörden führen vor diesem Hintergrund derzeit koordinierte Kontrollen bei Webseiten-Anbieter durch, um zu prüfen, ob die Datenschutzvorgaben für Drittlanddatentransfers beim Webseiten-Hosting und bei Einsatz von Webtracking eingehalten werden.

Bei Fragen zum Thema stehen Ihnen unsere Mitglieder der › **Praxisgruppe IP, IT und Datenschutz** gerne zur Verfügung.

AUTOREN

Janina Winz

Standort Düsseldorf

+49 211 600500-431

janina.winz@kapellmann.de

Dr. Inga Maaske

Standort Düsseldorf

+49 211 600500-402

inga.maaske@kapellmann.de