

Angepasster Datenschutz nach TTDSG?

Am 1. Dezember 2021 tritt das viel diskutierte TTDSG in Kraft. Wir haben uns die neuen Vorschriften angeschaut und für Sie hier zusammengefasst.

Worum geht es?

Das „Telekommunikations-Telemedien-Datenschutzgesetz“ (TTDSG) ist unter anderem auf den Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien sowie den Schutz der Privatsphäre durch Bestimmung von Anforderungen an die Speicherung von und Zugriff auf Informationen in Geräten der Nutzerinnen und Nutzer gerichtet. Notwendig wurde das TTDSG aus zweierlei Gründen: einerseits musste die **ePrivacy-Richtlinie** (RiLi 2002/58/EG in der durch die RiLi 2009/136/EG geänderten Fassung) endlich in das deutsche Recht umgesetzt, andererseits mussten die **Datenschutzbestimmungen** des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) an die Datenschutz-Grundverordnung (DSGVO) angepasst werden.

Für wen gilt das neue Recht?

Besonders betroffen von den neuen Regelungen sind Anbieter von Telemedien und Anbieter von Telekommunikationsdiensten.

„**Anbieter von Telemedien**“ ist gemäß § 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“. Telemedien werden im TTDSG nicht definiert, dafür aber im TMG: Gemäß § 1 Abs. 1 TMG sind alle **elektronischen Informations- und Kommunikationsdienste**, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind, Telemedien. Der Diensteanbieter von Telemedien ist gemäß § 2 Nr. 1 TMG „jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt“. Beispiele für Telemedien sind reichlich vorhanden: Websites, Informationsdienste, Soziale Medien, Suchmaschinen u.v.m.

„**Anbieter von Telekommunikationsdiensten**“ erbringen gemäß § 3 Nr. 24 TKG in der Regel gegen Entgelt solche Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Unter diese Begriffsbestimmung fallen unter anderem E-Mail-Diensteanbieter sowie Messenger wie etwa WhatsApp u.ä.

Was hat sich wesentlich verändert?

Zunächst die „**Good News**“: Die Rechtslage hinsichtlich der Vertraulichkeit der Kommunikation, Geheimhaltungspflichten, Verarbeitung von Verkehrsdaten oder Bereitstellung von Endnutzerdaten hat sich nicht verändert, vielmehr wurden die Regelungen an das ohnehin geltende Recht angepasst und in ein Gesetz zusammengeführt.

Änderungen ergeben sich im Bereich der sog. „**OTT-Kommunikation**“, sodass auch die Messenger-Dienste oder E-Mail-Anbieter unter die neuen Regelungen fallen, sowie im Bereich der Rechte von Endnutzererben (§ 4 TTDSG), deren Wahrnehmung trotz des Fernmeldegeheimnisses möglich sein muss.

Eine weitere Änderung bezieht sich auf die sog. „**Cookies**“ (das ist auch der Grund, warum das TTDSG vielerorts diskutiert wurde). Hier folgt der deutsche Gesetzgeber der DSGVO und postuliert ein Verbot mit Erlaubnisvorbehalt für die Verwendung von jeglichen Technologien, die eine Speicherung von Informationen in der „Endeinrichtung des Endnutzers“ (Endgerät wie etwa Handy, PC, Laptop etc.) oder einen Zugriff auf solche Informationen, die bereits in der Endeinrichtung gespeichert sind, ermöglichen. Diese Technologien sind also verboten, es sei denn „der Endnutzer [hat] auf der Grundlage von klaren und umfassenden Informationen eingewilligt“, § 25 Abs. 1 S. 1 TTDSG. Welche Informationen dabei zur Verfügung gestellt werden müssen sowie ob diese klar und umfassend sind misst sich dabei an den Vorschriften der DSGVO.

Die **Einwilligung** ist nach § 25 Abs. 2 TTDSG lediglich dann nicht erforderlich,

- wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die **Durchführung der Übertragung einer Nachricht** über ein öffentliches Telekommunikationsnetz ist

oder

- wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen **unbedingt erforderlich** ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Wie auch die DSGVO ist das TTDSG technologie-neutral, d.h. nicht nur solche Techniken wie Cookies oder Pixel, sondern auch andere Tracking-Methoden wie etwa Browser-Fingerprinting oder Werbe-ID sind davon mitumfasst.

Schließlich erwähnenswert sind im § 26 TTDSG vorgesehene „**anerkannte Dienste zur Einwilligungsverwaltung**, Endnutzereinstellungen“. Es geht dabei darum, dass Nutzerinnen und Nutzer über einen (zusätzlichen) Dienst nach ihren eigenen Vorstellungen bestimmen können, welche Tracking-Technologien in welchem Umfang unter welchen Voraussetzungen in dem von ihnen verwendeten Browser eingesetzt werden dürfen. Diese Dienste müssen dabei „von einer unabhängigen Stelle“ anerkannt werden, die die Bundesregierung noch zu bestimmen hat. Im gleichen Zuge wird die Bundesregierung die Anforderungen und das Verfahren für solche Anerkennung bestimmen müssen.

Die Kriterien für die Anerkennung solcher Dienste sind indes bereits im § 26 Abs. 1 TTDSG definiert:

- es geht um **nutzerfreundliche und wettbewerbskonforme Verfahren** und technische Anwendungen zur Einholung und Verwaltung der Einwilligung,
- Dienstanbieter dürfen **kein wirtschaftliches Eigeninteresse** an der Erteilung der Einwilligung und an den verwalteten Daten haben und unabhängig von Unternehmen sind, die ein solches Interesse haben können,
- die personenbezogenen Daten und die Informationen über die Einwilligungsentscheidungen dürfen für **keine anderen Zwecke** als die Einwilligungsverwaltung verarbeitet werden und
- ein **Sicherheitskonzept** muss vorgelegt werden, das eine Bewertung der Qualität und Zuverlässigkeit des Dienstes und der technischen Anwendungen ermöglicht und aus dem sich ergibt, dass der Dienst sowohl technisch als auch organisatorisch die **rechtlichen Anforderungen an den Datenschutz** und die Datensicherheit, die sich insbesondere aus **DSGVO** ergeben, erfüllt.

Wie genau die Anerkennung aussehen wird, bleibt noch abzuwarten.

Was ist zu tun?

Der erste Schritt sollte in Richtung der Überprüfung des Cookies-Einsatzes auf der eigenen Webseite sein. Denn ein fehlerhaftes und datenschutzrechtswidriges Nutzer:innen-Tracking ist leider immer noch weit verbreitet und kann zu Bußgeldern

sowohl wegen des Verstoßes gegen TTDSG, TMG oder TKG als auch wegen des Verstoßes gegen die DSGVO (kumulativ) führen.

Beispielsweise haben Datenschutzaufsichtsbehörden mehrerer Bundesländer im Sommer 2021 die Webseiten von Medienunternehmen auf die Rechtskonformität ihrer Verwendung von Cookies und Trackingtechnologien kontrolliert. Das Ergebnis war – leider – wenig überraschend: „Die meisten der geprüften Webseiten entsprechen nicht den rechtlichen Anforderungen für den Einsatz von Cookies und anderen Trackingtechniken“, so LDI NRW in der entsprechenden News-Veröffentlichung [hier](#). Insbesondere haben die Datenschutzaufsichtsbehörden festgestellt, dass personenbezogene Daten der Nutzerinnen und Nutzer zur Erstellung und Anreicherung umfassender und seitenübergreifender Persönlichkeitsprofile für die Zwecke des Onlinemarketings, insbesondere für Real Time Bidding-Verfahren (Echtzeitauktion von Werbeplätzen), verwendet werden, sowie dass die Einwilligungen von Nutzerinnen und Nutzern zwar angefordert werden, jedoch „in der Mehrheit der Fälle“ nicht rechtskonform gestaltet und somit auch unwirksam gewesen. Dabei konnten die an der Prüfung beteiligten Behörden folgende Mängel der Einwilligung(en) ermitteln:

- **„Erst tracken, dann fragen“**: Einwilligungsbedürftige Drittdienste und Cookies werden bereits beim Öffnen der Webseiten eingebunden bzw. gesetzt – also noch vor der Einwilligungsabfrage.
- **„Was ich nicht weiß, macht mich nicht heiß“**: Im Einwilligungsbanner werden nur unzureichende oder falsche Informationen über das Nutzertracking gegeben.
- **„Ich mag's nicht so kompliziert“**: Wird der Nutzerin oder dem Nutzer doch noch die Möglichkeit eingeräumt, alle Cookies und/oder andere Tracking-Technologien abzulehnen, und nimmt sie/er diese wahr, so bleiben dennoch zahlreiche Cookies und Drittdienste aktiv, die ebenfalls eine Einwilligung erfordern (doch keine bekommen haben).
- **„Nein ist keine Option“**: Eine Schaltfläche mit der Möglichkeit, eine Zustimmung zu sämtlichen Cookies und Drittdiensten zu erteilen, ist stets vorhanden; dagegen fehlt es häufig an einer ebenso einfachen Möglichkeit, sämtliche Cookies und Drittdienste abzulehnen.
- **„Schubsen gestattet“**: Nudging, also das unterschwellige Drängen zur Abgabe einer Einwilligung etwa durch farbliche Hervorhebung oder unnötige Verkomplizierung einer Ablehnung, stellt eine regelmäßig vorhandene Form der Manipulation dar und ist ebenso DSGVO-konform wie das gänzliche Fehlen eines Cookie-Banners.

All diese Beispiele zeigen eindrucksvoll, wie ein Unternehmen seine Cookies und andere Tracking-Dienste FALSCH einsetzen kann. Machen Sie es den überprüften Medienunternehmen nicht nach und gestalten Sie Ihre Dienste DSGVO-konform. Brauchen Sie dabei Unterstützung? Melde Sie sich gerne bei uns!

Haben Sie noch weitere Fragen hierzu? Melden Sie sich gerne bei unserer Expertin

Olga Kunkel (olga.kunkel@itwirtschaft.de)

Text: Olga Kunkel

Stand: 24.11.2021