Konferenz der unabhängigen Datenschutzaufsichtsbehörden

des Bundes und der Länder

Orientierungshilfe der Aufsichtsbehörden

für Anbieter:innen von digitalen Diensten (OH Digitale Dienste)

Version 1.2

Stand:

November 2024

Inhalt

I. Einführung

(1) Beim Betrieb von digitalen Diensten, wie insbesondere Webseiten und Apps, kommen regelmäßig Technologien – häufig von Drittdienstleistern[1] – zum Einsatz, die es ermöglichen, personenbezogene Daten von Nutzenden zu verschiedenen Zwecken zu verarbeiten. Ein sehr praxisrelevantes Beispiel solcher Technologien sind sog. Cookies. Mittels Cookies und ähnlicher Technologien können Informationen auf den Geräten der Nutzenden abgelegt, angereichert und verwaltet werden, die bei der Verwendung eindeutiger Kennungen (UIDs) eine Identifikation oder Zuordnung zu einer natürlichen Person zulassen. In der Praxis dienen diese Prozesse häufig dazu, das individuelle Verhalten der Nutzenden – zum Teil übergreifend über verschiedene Webseiten und Geräte – nachzuverfolgen und ggf. Profile über eine Person zu bilden.

(2) Unabhängig von der technischen Ausgestaltung oder den verfolgten Zwecken wird die Erhebung und weitere Verarbeitung dieser Informationen meist als ein einheitlicher Lebenssachverhalt wahrgenommen. Rechtlich sind hier jedoch zwei Schritte zu unterscheiden. Erstens die Speicherung von und der Zugriff auf Informationen in der Endeinrichtung sowie zweitens die Verarbeitung personenbezogener Daten, die oftmals mit dem Einsatz von Cookies und ähnlichen Technologien bezweckt wird. Die Rechtmäßigkeit dieser (Folge-)Verarbeitungen richtet sich nach den Anforderungen der Datenschutz-Grundverordnung (DS-GVO). Die vorgelagerten technischen Prozesse – insbesondere das Setzen und Auslesen von Cookies – berühren jedoch auch die Integrität der Endeinrichtungen und unterfallen damit originär in den Regelungsbereich der Richtlinie 2002/98/EG[2] in der durch die Richtlinie 2009/136/EG geänderten Fassung (sog. ePrivacy-RL[3]).

(3) Nach der Bewertung der Aufsichtsbehörden war der seit 2009 geltende Art. 5 Abs. 3 ePrivacy-RL für Telemedien durch § 15 des Telemediengesetzes (TMG) zunächst nicht hinreichend in nationales Recht umgesetzt worden. Zudem ergaben sich Schwierigkeiten in der Anwendung seit der Geltung der DS-GVO. Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) hatte vor diesem Hintergrund im März 2019 die „Orientierungshilfe für Anbieter von Telemedien“ (OH Telemedien 2019) veröffentlicht, die diesen helfen sollte, die rechtlichen Anforderungen umzusetzen.

(4) Mit Wirkung zum 1. Dezember 2021 war Art. 5 Abs. 3 ePrivacy-RL zunächst durch § 25 Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG)[4] in deutsches Recht umgesetzt worden. Die Anforderungen des § 25 TTDSG waren beim Einsatz von jeglichen Technologien zu beachten, mittels derer

---

[1] Wenn in diesem Text oder etwaigen Anlagen Bezeichnungen wie „Dritte“ „Drittdienstleister“ oder „Drittanbieter“ verwendet werden, ist dies nicht im Sinne von Art. 4 Nr. 10 DS-GVO zu verstehen, so dass Auftragsverarbeiter und deren Dienste eingeschlossen sind.

[2] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

[3] Sofern im Folgenden eine Vorschrift der ePrivacy-Richtlinie genannt wird, ist immer die aktuelle gemeint in der Fassung der Änderungen durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

[4] Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23. Juni 2021 (BGBl. 2021 I 1982).

Informationen auf Endeinrichtungen gespeichert oder aus diesen ausgelesen werden. Mit Blick auf diese Änderung wurde die OH Telemedien im Jahr 2021 vollständig überarbeitet und ergänzt.[5]

(5) Gemäß Art. 8 Änderungsgesetz zur Einführung des Digitale-Dienste-Gesetzes wurde der Begriff „Telemedien“ im TTDSG nunmehr durch den Begriff „digitale Dienste“ ersetzt, sodass das Gesetz nunmehr Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) heißt.[6] Gleichzeitig mit dem Inkrafttreten des Digitale-Dienste-Gesetz (DDG) zum 14.05.2024 ist das TMG ganz außer Kraft getreten.[7]

(6) Der neue § 25 TDDDG entspricht inhaltlich der Vorgängernorm des § 25 TTDSG. Die OH Digitale Dienste ist an die neue Terminologie angepasst. Zudem wurden Aktualisierungen in den Rz. 114 ff. vorgenommen, um Rechtsentwicklungen seit 2021 abzubilden.

(7) Die nachfolgend dargestellten Anforderungen und Wertungen sind nicht auf den Betrieb von Webseiten und Apps beschränkt, jedoch stellen diese die häufigsten Anwendungsfälle dar. Daher finden sich in den Ausführungen vorwiegend Beispiele zur Veranschaulichung aus diesen Anwendungsbereichen.

(8) Die Orientierungshilfe ergänzt die EDSA Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive.

II. Anwendungsbereich des TDDDG

(9) Das TDDDG regelt unter anderem den Schutz der Privatsphäre bei der Nutzung von Endeinrichtungen, unabhängig davon, ob ein Personenbezug vorliegt oder nicht. Daneben enthält das Gesetz besondere Vorschriften zu technischen und organisatorischen Vorkehrungen, die von Anbieter:innen digitaler Dienste zu beachten sind, und die Anforderungen an die Erteilung von Auskünften über Bestands- und Nutzungsdaten. Anlass der Gesetzgebung des TTDSG war die Richtlinie 2018/1972/EU über den europäischen Kodex für die elektronische Kommunikation[8], die eine Änderung des TKG erforderlich machte. Der Gesetzgeber nahm dabei die Gelegenheit wahr, die bis 2021 nicht an die DS-GVO angepassten Datenschutzvorschriften des TKG und des damaligen TMG ebenfalls in den Blick zu nehmen und im heutigen TDDDG zusammenzuführen.[9] Ziel war es, beide Bereiche an die DS-GVO und die ePri-

[5] Beschluss der Datenschutzkonferenz vom 20. Dezember 2021, https://datenschutzkonferenz-online.de/orientierungshilfen.html

[6] Artikel 8 des Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze vom 06.05.2024 (BGBl. 2024 I Nr. 149).

[7] Art. 37 des Gesetzes zur Durchführung der Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG sowie zur Durchführung der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten und zur Änderung weiterer Gesetze vom 06.0506.05.2024 (BGBl. 2024 I Nr. 149).

[8] Richtlinie 2018/1972/EU des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation.

[9] Gesetz zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) vom 23. Juni 2021 (BGBl. 2021 I 1858). Ein Restbestand des TMG blieb dabei erhalten, das TKG wurde neu erlassen.

vacy-RL anzupassen und insbesondere die Vorgaben aus Art. 5 Abs. 3 ePrivacy-RL rechtssicher in nationales Recht umzusetzen.[10] Nach den ursprünglichen Plänen der Europäischen Kommission sollte zeitgleich mit der DS-GVO eine europäische Verordnung über Privatsphäre und elektronische Kommunikation (ePrivacy-Verordnung) in Kraft treten und die ePrivacy-RL ersetzen. Bis zum Veröffenlichungsdatum dieser Orientierungshilfe ist jedoch noch immer nicht absehbar, ob und wann es eine solche ePrivacy-Verordnung geben wird. Sollte es hierzu kommen, würde das TDDDG von der Verordnung als höherrangigem Recht mit unmittelbarer Wirkung weitgehend abgelöst werden.

1. Adressaten

(10) Adressaten des TDDDG sind neben den Anbieter:innen von Telekommunikationsdiensten vor allem Anbieter:innen von digitalen Diensten gemäß § 2 Abs. 2 Nr. 1 TDDDG. Hierunter fällt jede natürliche oder juristische Person, die eigene oder fremde digitale Dienste erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden digitalen Diensten vermittelt. Diese Definition weicht in der Formulierung etwas von der Definition des „Diensteanbieters“ gemäß § 1 Abs. 42 Nr. 51 DDG ab. Danach ist ein Diensteanbieter schlicht „jeder Anbieter digitaler Dienste“.

(11) Digitale Dienste sind gemäß § 2 Abs. 1 TDDDG i.V. m. § 1 Abs. 4 Nr. 1 i.V.m. Art. 1 Abs. 1 lit. b der Richtlinie (EU) 2015/1535 Richtlinie (EU) 2015/1535 eine Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung.

2. Räumlicher Anwendungsbereich

(12) Nach § 1 Abs. 3 unterliegen alle Adressaten dem TDDDG, die im Geltungsbereich des Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. Laut Gesetzesbegründung *„gilt nach wie vor das Marktortprinzip. Die im Verhältnis zur E-Privacy-Richtlinie subsidiär geltende DSGVO enthält bereits das Marktortprinzip, das damit auch für die Verarbeitung von personenbezogenen Daten durch Telekommunikationsanbieter gilt. Im Hinblick auf die Verarbeitung von personenbezogenen Daten durch Anbieter von Telemedien gilt das Marktortprinzip der DSGVO ebenfalls unmittelbar*“.[11]

3. Abgrenzung der Anwendungsbereiche des TDDDG und der DS-GVO

(13) Nach Art. 2 Abs. 1 gilt die DS-GVO – mit Ausnahmen – für „die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“. Die ePrivacy-RL – und damit auch die nationale Umsetzung im TDDDG – zielt gemäß Art. 1 Abs. 1 und 2 u. a. auf einen gleichwertigen Schutz des Rechts auf Privatsphäre und Vertraulichkeit ab und bezweckt eine

[10] BT-Drs. 19/27441, Gesetzesbegründung der Bundesregierung, S. 30.
[11] BT-Drs. 19/27441, S. 34.

„Detaillierung und Ergänzung“ der Bestimmungen der DS-GVO in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation.

(14) Im Rahmen des Angebots von digitalen Diensten gibt es Vorgänge, die nur in den Anwendungsbereich eines der beiden Regelungsmaterien fallen.[12] Werden durch den Einsatz von Technologien beispielsweise keine personenbezogenen Daten verarbeitet, sind nur die Vorgaben des TDDDG, nicht aber diejenigen der DS-GVO zu beachten.[13] Regelmäßig werden jedoch Prozesse in Rede stehen, wie beispielsweise der Einsatz von Cookies zur Nachverfolgung des Verhaltens von Nutzenden, bei denen auch eine Verarbeitung personenbezogener Daten erfolgt und damit die Anwendungsbereiche sowohl des TDDDG als auch der DS-GVO eröffnet sind. Für diesen Fall enthält Art. 95 DS-GVO eine Kollisionsregel. Danach werden datenverarbeitenden Stellen durch die DS-GVO keine zusätzlichen Pflichten auferlegt, soweit sie besonderen in der ePrivacy-RL festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen. Diese Kollisionsregel entfaltet Geltung auch für die nationalen Umsetzungsnormen der Richtlinie, wie das TDDDG.

(15) Mithin gelten die spezifischen Bestimmungen des § 25 TDDDG vorrangig vor den Bestimmungen der DS-GVO, soweit beim Speichern und Auslesen von Informationen in Endeinrichtungen personenbezogene Daten verarbeitet werden. Für die nachfolgenden Verarbeitungen personenbezogener Daten, die erst durch das Auslesen dieser Daten vom Endgerät ermöglicht und die von keiner Spezialregelung erfasst werden, sind wiederum die allgemeinen Vorgaben der DS-GVO zu beachten.

III. Schutz der Privatsphäre in Endeinrichtungen gemäß § 25 TDDDG

(16) Die zentrale Norm des TDDDG mit Bezug auf die hier zu betrachtenden Technologien stellt die Regelung des § 25 TDDDG dar. § 25 TDDDG dient – anders als die Vorschriften der DS-GVO – dem Schutz der Privatsphäre und Vertraulichkeit bei der Nutzung von Endeinrichtungen. Endnutzer:innen werden also davor geschützt, dass Dritte unbefugt auf deren Endeinrichtung Informationen speichern oder auslesen und dadurch ihre Privatsphäre verletzen.

1. Gegenstand und Anwendungsbereich von § 25 TDDDG

(17) Nachfolgend werden der Anwendungsbereich und die Regelungssystematik der Vorschrift dargestellt. Ein Schwerpunkt der Ausführungen liegt bei der Bewertung, in welchen Fällen eine Einwilligung gemäß § 25 Abs. 1 TDDDG erforderlich ist und in welchen Fällen die Ausnahmeregelungen gemäß § 25 Abs. 2 TDDDG greifen können.

---

[12] Nähere Ausführungen nebst Beispielen hierzu sind der EDSA Stellungnahme 5/2019 zum Zusammenspiel zwischen der ePrivacy-Richtlinie und der DS-GVO, insbesondere in Bezug auf die Zuständigkeiten, Aufgaben und Befugnisse von Datenschutzbehörden vom 12. März 2019, ab Rn. 21, zu entnehmen.

[13] S. sogleich unter III.1.

a) Grundsatz der Einwilligungsbedürftigkeit

(18) § 25 Abs. 1 Satz 1 TDDDG normiert den Grundsatz, dass die Speicherung von Informationen in der Endeinrichtung von Nutzenden oder der Zugriff auf solche Informationen, die bereits in der Endeinrichtung gespeichert sind, nur mit Einwilligung der Endnutzer:innen zulässig sind.

b) Endeinrichtungen

(19) Für die Eröffnung des Anwendungsbereichs der Norm wird nicht unmittelbar an einen Telekommunikations- oder digitalen Dienst angeknüpft, sondern auf die Endeinrichtungen abgestellt – entsprechend lautet auch die Überschrift des Kapitels, zu dem § 25 TDDDG gehört, „Endeinrichtungen".

(20) Endeinrichtungen werden in § 2 Abs. 2 Nr. 6 TDDDG legaldefiniert als „jede direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über Draht, optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Endeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet." Der Gesetzesbegründung ist zu entnehmen, dass dieser weite Anwendungsbereich bewusst gewählt wurde, um nicht nur die Kommunikation via klassischer Telefonie und Internet (Voice-over-IP) zu erfassen, sondern auch die Vielzahl von Gegenständen, die inzwischen – kabelgebunden oder über WLAN-Router – an das öffentliche Kommunikationsnetz angeschlossen sind.[14] Über Laptops, Tablets oder Mobiltelefone hinaus betrifft dies auch den Bereich des Internet der Dinge (Internet of Things, IoT), z. B. Smarthome-Anwendungen wie Küchengeräte, Heizkörperthermostate oder Alarmsysteme, sowie Smart-TVs oder auch vernetzte Fahrzeuge, wenn und soweit diese über die entsprechenden Kommunikationsfunktionen verfügen. Seine Grenze findet der Anwendungsbereich, wo technische Einrichtungen nicht mit dem „Internet" als öffentlichem Telekommunikationsnetz verbunden sind (bspw. isolierte Firmennetzwerke).[15]

c) Speicherung und Zugriff auf Informationen

(21) Gemäß § 25 Abs. 1 S. 1 TDDDG bedarf die Speicherung von Informationen in der Endeinrichtung oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, der Einwilligung der Endnutzer:innen. Die Vorschrift ist diesbezüglich technikneutral formuliert, so dass alle Techniken und Verfahren erfasst werden, mittels derer das Speichern und Auslesen von Informationen erfolgen kann. Art. 5 Abs. 3 ePrivacy-RL in der Fassung vom 12. Juli 2002 verfolgte das Ziel, so genannte „Spyware", „Web-Bugs", „Hidden Identifiers", „Cookies" und ähnliche Instrumente zu regulieren, mittels derer ohne das Wissen des Nutzers in dessen Endgerät eingedrungen werden kann, um Zugang zu Informationen zu erlangen oder die Nutzeraktivität zurückzuverfolgen.[16] Bei der Neuregelung von Art. 5 Abs. 3 ePrivacy-RL im Jahr 2009 wurden als konkrete Beispiele Cookies, Spähsoftware oder Viren aufgeführt.[17] Im allgemeinen und auch im juristischen Sprachgebrauch wird Art. 5 Abs. 3 ePrivacy-RL häufig

[14] BT-Drs. 19/27441, S. 38.
[15] BT-Drs. 19/27441, S. 38.
[16] S. Erwägungsgrund 24 f. der ePrivacy-RL.
[17] S. Erwägungsgrund 66 der ePrivacy-RL.

stark verkürzt nur als Cookie-Regelung bezeichnet, da Cookies die wohl in der Praxis bisher bedeutendste Möglichkeit zur Speicherung und zum Auslesen von Informationen sind. Eine Speicherung von Informationen im Sinne der Vorschrift erfolgt im Webseitenkontext darüber hinaus z. B. auch durch Web-Storage-Objekte (Local- und Session-Storage-Objekte).

(22) Außerhalb des Webseitenkontextes können insbesondere automatische Update-Funktionen von Hard- oder Software zu einer Speicherung oder zu einem Auslesen von Informationen auf den Endgeräten führen, mit der Folge, dass nach § 25 Abs. 1 TDDDG eine Einwilligung erforderlich ist. Bei mobilen Endgeräten sind als besonders praxisrelevante Fälle der Zugriff auf Hardware-Gerätekennungen, Werbe-Identifikationsnummern, Telefonnummern, Seriennummern der SIM-Karten (IMSI), Kontakte, Anruflisten, Bluetooth-Beacons oder die SMS-Kommunikation zu nennen. Bei allen Geräten ist zudem das Auslesen der eindeutigen Kennungen der Netzwerk-Hardware (MAC-Adressen) zu berücksichtigen.

(23) Ebenso kommt mittlerweile häufig das sogenannte Browser-Fingerprinting zum Einsatz. Dies bezeichnet den Prozess der serverseitigen Bildung eines möglichst eindeutigen und langlebigen (Hash-)Werts oder Abbildes als Ergebnis einer mathematischen Berechnung von Browser-Informationen, wie beispielsweise Bildschirmauflösungen, Betriebssystemversionen oder installierte Schriften.

(24) Auch ist es als Zugriff von Informationen auf Endeinrichtungen der Endnutzer:innen zu werten, wenn aktiv – beispielsweise mittels JavaScript-Code – Eigenschaften eines Endgerätes ausgelesen und für die Erstellung eines Fingerprints an einen Server übermittelt werden.[18]

(25) Die Verarbeitung der übermittelten Browser-Informationen zu einem Fingerprint und dessen Verwendung zu bestimmten Zwecken ist in beiden Fällen nicht ohne Weiteres zulässig, sondern muss, wenn es zu einer Verarbeitung personenbezogener Daten kommt, den Anforderungen der DS-GVO gerecht werden.

d) Kein Personenbezug erforderlich

(26) Im Unterschied zu den datenschutzrechtlichen Vorschriften begründet § 25 Abs. 1 TDDDG ein Einwilligungserfordernis für das Speichern und/oder Auslesen von Informationen auf bzw. aus einem Endgerät unabhängig von einem Personenbezug der Informationen. Damit wird bereits durch den Wortlaut der Vorschrift deutlich gemacht, dass sie über den Anwendungsbereich der DS-GVO hinausgeht.

(27) Der BGH hat in seiner Entscheidung „Planet49“ vom 28. Mai 2020 bezogen auf die Abgrenzung des Regelungsbereichs von Art. 5 Abs. 3 ePrivacy-RL zur DS-GVO Folgendes ausgeführt:

> *„Art. 5 Abs. 3 der RL 2002/58/EG betrifft nicht den Regelungsgegenstand der VO (EU) 2016/679, gemäß ihres Art. 1 Abs. 1 DS-GVO die Verarbeitung personenbezogener Daten, sondern die Speicherung von oder den Zugriff auf Informationen, die im Endgerät des Nutzers gespeichert sind. Dieser Unterschied im Anwendungsbereich hat seinen Grund in den unterschiedlichen Schutzzwecken der betroffenen Regelungen: Während die VO (EU) 2016/679 nach ihrem Art. 1 Abs. 2 DS-GVO und ihren Erwägungsgründen 1 und 2 die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren in Art. 8 GRCh gewährleistetes Recht auf Schutz personenbezogener Daten schützt, dient Art. 5 Abs. 3 der RL 2002/58/EG, wie sich aus*

[18] Zur Anwendung der ePrivacy-RL auf das Browserfingerprinting s. bereits Art. 29-Datenschutzgruppe, Anwendung der Richtlinie 2002/58/EG auf die Nutzung des virtuellen Fingerabdrucks (WP 224).

ihren Erwägungsgründen 24 und 25 und den Erwägungsgründen 65 und 66 der diese Richtlinie ändernden RL 2009/136/EG ergibt, dem durch Art. 8 Abs. 1 EMRK und (inzwischen) durch Art. 7 GRCh garantierten Schutz der Privatsphäre der Nutzer. Art. 5 Abs. 3 der RL 2002/58/EG soll den Nutzer vor jedem Eingriff in seine Privatsphäre schützen, unabhängig davon, ob dabei personenbezogene Daten oder andere Daten betroffen sind […]. Mithin geht die Regelung des Art. 5 Abs. 3 der RL 2002/58/EG über den Anwendungsbereich der VO (EU) 2016/679 hinaus."[19]

(28) Da § 25 TDDDG die Vorgaben des Art. 5 Abs. 3 ePrivacy-RL ins deutsche Recht umsetzen soll, gelten die gleichen Erwägungen für die Abgrenzung der nationalen Vorschrift zur DS-GVO. Für den Einsatz von Cookies bedeutet dies beispielsweise, dass das Einwilligungserfordernis nach § 25 TDDDG unabhängig davon greift, ob in dem Cookie personenbezogene Daten, z. B. in Form einer eindeutigen Identifizierungsnummer, gespeichert sind oder auf diese zugegriffen werden soll.

e) Bündelung von Einwilligungen

(29) Die Einwilligung in das Speichern und Auslesen von Informationen, die nach § 25 Abs. 1 TDDDG erforderlich ist, und die Einwilligung, die als Rechtsgrundlage für eine geplante weitere Verarbeitung der ausgelesenen Daten gemäß Art. 6 Abs. 1 lit. a) DS-GVO erforderlich sein kann, können unter Berücksichtigung der nachfolgenden Bedingungen durch dieselbe Handlung[20] erteilt werden.[21] Dies setzt allerdings voraus, dass die Anbieter:innen des digitalen Dienstes die Nutzenden bereits an dieser Stelle über alle Zwecke einer Datenverarbeitung informieren, die im Anschluss an den Zugriff auf die Endeinrichtung erfolgen sollen. Hierbei ist darauf zu achten, dass bei der Abfrage eindeutig erkennbar sein muss, dass mit einer einzelnen Handlung, bspw. dem Betätigen einer Schaltfläche,[22] mehrere Einwilligungen erteilt werden. Werden Nutzende, z. B. mittels eines Banners, auf einer Webseite darum gebeten, eine Einwilligung in den Einsatz von Cookies zu erteilen, ohne dass im Wortlaut der Einwilligung auch die Folgeverarbeitungen angesprochen werden, so handelt es sich nicht um eine gebündelte Einwilligung nach TDDDG und DS-GVO, sondern lediglich um eine Einwilligung nach dem TDDDG.

2. Anforderungen an die Einwilligung

(30) Das TDDDG selbst enthält im Unterschied zu den früheren Regelungen in § 94 TKG a. F. und § 13 Abs. 2 TMG a. F. keine spezifischen Vorgaben für die Einwilligung. § 25 Abs. 1 S. 2 TDDDG verweist sowohl bezüglich der Informationspflichten gegenüber den Endnutzer:innen als auch der formalen und inhaltlichen Anforderungen an eine Einwilligung auf die DS-GVO. Maßgeblich ist somit die Definition nach Art. 4 Nr. 11 DS-GVO. Die weiteren Anforderungen an eine wirksame Einwilligung ergeben sich aus Art. 7 und Art. 8 DS-GVO.[23] Für die Beurteilung der Wirksamkeit einer Einwilligung gemäß § 25 Abs. 1 S. 1

---

[19] BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 Rn. 61 – Cookie-Einwilligung II (Planet49).
[20] EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, Fn. 17.
[21] Zur Abgrenzung der Prozesse, siehe bereits oben unter I. und II.2.
[22] Unter Schaltfläche ist im Kontext dieser Orientierungshilfe jede interaktive Möglichkeit zu verstehen, mit der Endnutzer:innen eine Erklärung abgeben können, z. B. mittels Schieberegler, Auswahlfeld, Kästchen oder Button.
[23] Die Anwendung dieser Vorschriften der DS-GVO steht im Einklang mit den europäischen Vorgaben, denn Art. 2 S. 2 lit. f) der ePrivacy-RL verweist für die Definition der Einwilligung auf Art. 2 lit. h) Datenschutz-RL. Bei der Berücksichtigung dieses

TDDDG sind demnach dieselben Bewertungsmaßstäbe anzulegen, wie bei einer Einwilligung nach Art. 6 Abs. 1 lit. a) DS-GVO.

(31) Den folgenden Ausführungen liegen somit zwar die genannten Vorschriften der Datenschutz-Grundverordnung zugrunde, konkretisierende Ausführungen und Beispiele beziehen sich aber auf § 25 Abs. 1 TDDDG.

(32) Eine Einwilligung ist entsprechend Art. 4 Nr. 11 DS-GVO jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Art. 7 und 8 DS-GVO stellen zudem weitere Bedingungen u. a. für den Widerruf und für Einwilligungen von Kindern auf.

(33) Aus diesen rechtlichen Vorgaben ergeben sich im Wesentlichen die folgenden Prüfungspunkte für die Beurteilung der Wirksamkeit einer Einwilligung im Kontext von § 25 Abs. 1 TDDDG:

- Einwilligung der Endnutzer:innen des Endgeräts,
- Zeitpunkt der Einwilligung,
- Informiertheit der Einwilligung,
- unmissverständliche und eindeutig bestätigende Handlung,
- bezogen auf den bestimmten Fall,
- Freiwilligkeit der Willensbekundung,
- Möglichkeit zum Widerruf der Einwilligung, die ebenso einfach sein muss wie die Erteilung.

(34) Nachfolgend werden diese Merkmale der Einwilligung in Bezug auf die Einwilligung gemäß § 25 Abs. 1 TDDDG näher erläutert.

a) Einwilligung der Endnutzer:innen der Endeinrichtung

(35) Gemäß § 25 TDDDG ist die Einwilligung der Endnutzer:innen des Endgeräts erforderlich. Im TDDDG ist keine Begriffsbestimmung von „Endnutzer“ oder „Endnutzerin“ enthalten. Der Begriff stammt aus dem Telekommunikationsrecht und wird beispielsweise auch in § 6 TDDDG verwendet. Entsprechend werden Endnutzer:innen in § 3 Nr. 13 TKG, der nach § 2 Abs. 1 TDDDG auch im TDDDG gilt, legaldefiniert als Nutzende, die weder öffentliche Telekommunikationsnetze betreiben noch öffentlich zugängliche Telekommunikationsdienste erbringen. Der Begriff des Endnutzers dient im Telekommunikationsrecht vor allem der Abgrenzung zu Anbieter:innen von Telekommunikationsdiensten, nicht aber zur Spezifizierung oder gar Eingrenzung des persönlichen Anwendungsbereichs von § 25 TDDDG. Im Unterschied zum Datenschutzrecht wird keine subjektive „Betroffenheit“ gefordert. Erforderlich ist vielmehr die Einwilligung von der Person, die objektiv die Endeinrichtung nutzt. Eigentumsverhältnisse in Bezug auf das Endgerät sind grundsätzlich ebenso irrelevant wie die Frage, wer Vertragspartner:in der Telekommunikationsdienstleistung ist, die mittels des Endgeräts in Anspruch genommen wird.

Verweises ist zu beachten, dass die Datenschutz-RL durch Art. 94 Abs. 1 DS-GVO mit Wirkung vom 25. Mai 2018 aufgehoben worden ist. Seither gelten gemäß Art. 94 Abs. 2 DS-GVO Verweise auf die aufgehobene Richtlinie als Verweise auf die DS-GVO.

b) Zeitpunkt der Einwilligung

(36) Zunächst ist darauf zu achten, dass eine entsprechende Willenserklärung bereits erteilt sein muss, bevor der einwilligungsbedürftige Zugriff auf die Endeinrichtung erfolgt. Es ist dementsprechend nicht zulässig, wenn einwilligungsbedürftige Cookies bereits mit dem erstmaligen Aufruf einer Website gesetzt und erst anschließend die Einwilligung abgefragt wird.

c) Informiertheit der Einwilligung

(37) Die Einwilligung ist in informierter Weise einzuholen. Welche Informationen konkret zu erteilen sind, ergibt sich – im Unterschied zu der Aufzählung von erforderlichen Informationen gemäß Art. 13 DS-GVO – nicht unmittelbar aus dem Gesetz[24]. Das Merkmal der „Informiertheit" setzt mindestens voraus, dass jegliche Speicher- und Ausleseaktivitäten transparent und nachvollziehbar sein müssen. Dies bedeutet im Kontext des § 25 Abs. 1 TDDDG, dass Nutzende u. a. Kenntnis darüber erhalten müssen, wer auf die jeweilige Endeinrichtung zugreift, in welcher Form und zu welchem Zweck, welche Funktionsdauer die Cookies haben und ob Dritte Zugriff darauf erlangen können.[25] Hierzu ist es auch erforderlich, dass bereits beim Zugriff auf die Endeinrichtung hinreichend darüber informiert wird, ob und ggf. inwieweit der Zugriff weiteren Datenverarbeitungsprozessen dient, die den Anforderungen der DS-GVO unterfallen, wobei die konkreten Zwecke der Folgeverarbeitung präzise zu beschreiben sind.[26] Um die Auswirkungen der Erteilung der Einwilligung zu verdeutlichen, muss schließlich auch über die Tatsache informiert werden, dass ein späterer Widerruf sich gemäß Art. 7 Abs. 3 S. 3 DS-GVO nicht mehr auf die Rechtmäßigkeit des bis zum Widerruf erfolgten Zugriffs bzw. der bis dahin erfolgten Speicherung auswirkt.

(38) Die Informationserteilung kann grundsätzlich über ein mehrstufiges Konzept, einen sog. layered approach erfolgen, sodass Nutzer:innen alle Informationen über mehrere Ebenen oder über eine Verlinkung zur Datenschutzerklärung erhalten können. Jedoch ist zu beachten, dass die Grundinformationen im Hinblick auf § 25 Abs. 1 TDDDG und/oder Art. 6 Abs. 1 lit. a) DS-GVO auf der Ebene erteilt werden müssen, auf der eine Einwilligung eingeholt werden soll.[27]

(39) Im Zusammenhang mit Webseiten und Apps besteht oftmals ein Defizit darin, dass die Banner, mit denen eine Einwilligung eingeholt werden soll, intransparent gestaltet sind, sodass u. a. die Zwecke des Zugriffs auf ein Endgerät und die beteiligten Akteure[28] nicht ausreichend erkennbar sind. Intransparenz kann sich auch daraus ergeben, dass unklar ist, mit welcher Schaltfläche welcher Effekt erreicht

---

[24] Die Formulierung „Information des Endnutzers" in § 25 Abs. 1 S. 2 TDDDG verweist auf die Informationspflichten gemäß Artikel 13 und 14 der DS-GVO.

[25] EuGH, Urteil vom 1. Oktober 2019 – C-673/17 – Planet49, Rn. 75 ff.

[26] EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, S. 16, ab Rn. 49.

[27] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, V.1.1 Rn. 74 Beispiel 13.

[28] Der Begriff „Akteure" bezieht sich im Kontext des TDDDGauf diejenigen, die Zugriff auf die Informationen der Endeinrichtung nehmen und diejenigen, die Informationen in der Endeinrichtung speichern. Dies sind im Regelfall der Webseitenbetreiber und gegebenenfalls Dritte, die ebenfalls Zugriff haben, beispielsweise Anbieter der eingesetzten Dienste. Sofern ein Zugriff auf die Endeinrichtung durch einen Drittdienstleister erfolgt, ist dieser daher als Akteur zu nennen, unabhängig davon, ob er eine nachfolgende Verarbeitung in eigener Verantwortung vornimmt oder ob er diese als Auftragsverarbeiter durchführt. Im Hinblick auf die DS-GVO wird hierfür auf die EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 65 verwiesen.

werden kann und wie oder mit welchem Aufwand eine Ablehnung von einwilligungsbedürftigen Prozessen möglich ist.

(40) Transparenz setzt auch voraus, dass die Informationen, die innerhalb eines digitalen Angebots an verschiedenen Stellen zur Verfügung gestellt werden, kongruent sind. In der Praxis fallen regelmäßig Webseiten und Apps auf, in deren Bannern zur Einwilligungsabfrage andere Informationen enthalten sind als in der Datenschutzerklärung, insbesondere andere Rechtsgrundlagen, andere Drittanbieter, andere Zwecke.

(41) Art. 7 Abs. 2 DS-GVO stellt besondere Transparenzanforderungen, wenn die Einwilligung durch eine „schriftliche Erklärung, die noch andere Sachverhalte betrifft", eingeholt wird. In Erwg. 32, S. 1 DS-GVO wird diesbezüglich ausgeführt, dass die schriftliche Erklärung auch elektronisch erteilt werden kann. Daher greift die besondere Transparenzanforderung grundsätzlich auch für Einwilligungsbanner. „Andere Sachverhalte" als die datenschutzrechtliche Einwilligung sind insbesondere dann betroffen, wenn über den Einwilligungsbanner gleichzeitig eine Einwilligung gemäß § 25 Abs. 1 TDDDG eingeholt werden soll. In diesem Fall muss das Ersuchen um die Einwilligungen in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache erfolgen und es muss erkennbar sein, dass zwei Einwilligungen erteilt werden – eine auf der Grundlage von § 25 Abs. 1 TDDDG und eine gemäß Art. 6 Abs. 1 lit. a.) DS-GVO.

(42) Anbieter:innen von digitalen Diensten, die ihre Datenschutzinformationen mit Blick auf § 25 TDDDG aktualisieren, müssen daher darauf achten, die Vorgänge klar zu differenzieren – wenn im Rahmen des digitalen Angebotes Prozesse stattfinden, die sowohl unter das TDDDG als auch unter die DS-GVO fallen, ist über die beiden Rechtsgrundlagen jeweils separat zu informieren.

d) Unmissverständliche und eindeutig bestätigende Handlung

(43) Art. 4 Nr. 11 DS-GVO setzt für eine wirksame Einwilligung zudem eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung" oder eine sonstige eindeutige bestätigende Handlung voraus, mit der die Nutzenden zu verstehen geben, dass sie mit dem Zugriff auf und dem Abruf von Informationen ausdrücklich einverstanden sind. Es bedarf mithin stets eines aktiven Handelns der Endnutzer:innen. Dies kann beispielsweise durch Anklicken einer designierten Schaltfläche in einem Banner, durch die Auswahl technischer Einstellungen oder durch eine andere Erklärung oder aktive Verhaltensweise geschehen, mit der die Endnutzer:innen eindeutig ihr Einverständnis hinsichtlich der Speicherung von oder den Zugriff auf Informationen in der Endeinrichtung ausdrücken.

(44) Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der Nutzenden können demgegenüber keine Einwilligung darstellen.[29] Opt-Out-Verfahren sind daher stets ungeeignet, eine wirksame Einwilligung zu begründen. Der Umstand, dass der Browser der Endnutzer:innen Cookies oder Web-Storage, z. B. Local Shared Objects (LSO) zulässt, kann dementsprechend auch – ungeachtet weiterer Aspekte wie Informiertheit oder Bestimmtheit – keine Einwilligung darstellen.[30]

[29] S. Erwägungsgrund 32 der DS-GVO.

[30] Erwägungsgrund 32 S. 2 betrifft dagegen den umgekehrten Fall, dass der Nutzer nachweisbar Browsereinstellungen vorgenommen, insbesondere die DNT-Einstellung aktiviert hat („DNT:0" = Tracking okay; „DNT:1" = kein Tracking).

(45) Die reine weitere Nutzung einer Webseite oder App, z. B. durch Handlungen wie das Herunterscrollen, das Surfen durch Webseiteninhalte, das Anklicken von Inhalten oder ähnliche Aktionen können - ungeachtet der weiteren Anforderungen an eine wirksame Einwilligung - ebenfalls keine wirksame Einwilligung für den Zugriff auf oder die Speicherung von Informationen auf einer Endeinrichtung darstellen. Diese Handlungen können keinesfalls den Einsatz von einwilligungsbedürftigen Cookies oder ähnlichen Technologien legitimieren – selbst wenn mittels eines Banners über die Prozesse informiert wird. Das Scrollen oder Weitersurfen sind typische Handlungen bei der Nutzung des Internets, denen grundsätzlich kein rechtlicher Erklärungsgehalt innewohnt. Art. 4 Nr. 11 DS-GVO fordert ausdrücklich eine eindeutige bestätigende Handlung, so dass eine Aktivität oder Interaktion der Nutzenden erforderlich ist, die eine klare Zäsur bei der weiteren Nutzung des digitalen Angebots zum Ausdruck bringt.[31] Nur dann können die verschiedenen Handlungen deutlich voneinander unterschieden und eine eindeutige Zustimmung festgestellt werden.

(46) Ob eine unmissverständliche Willenserklärung vorliegt, wenn Endnutzer:innen ihre Einwilligung über eine Schaltfläche abgegeben haben, hängt auch davon ab, ob diese ihren wahren Willen unmittelbar zum Ausdruck bringen konnten oder eindeutig erkennen konnten, wie der wahre Wille zum Ausdruck gebracht werden kann. In die Bewertung fließt daher mit ein, wie die Schaltflächen für die Abgabe der Einwilligung und weitere Handlungsoptionen beschriftet und gestaltet sind und welche Zusatzinformationen zur Verfügung gestellt werden.

(47) Wenn in digitalen Diensten Einwilligungsbanner angezeigt werden, die lediglich eine „Okay“-Schaltfläche enthalten, stellt das Anklicken der Schaltfläche keine unmissverständliche Erklärung dar. Auch die Bezeichnungen „Zustimmen“, „Ich willige ein“ oder „Akzeptieren“ können im Einzelfall nicht ausreichend sein, wenn aus dem begleitenden Informationstext nicht eindeutig hervorgeht, wozu konkret die Einwilligung erteilt werden soll. Häufig müssen Nutzende zunächst eine im Einwilligungsbanner integrierte Detailansicht öffnen, um darüber zu sehen, welche Voreinstellungen im Falle eines Klicks auf „Akzeptieren“ gesetzt sind und daraus abzuleiten, worauf sich die Einwilligung letztlich bezieht. Derartige Gestaltungen stehen einer wirksamen Einwilligung regelmäßig ebenfalls entgegen.

(48) Darüber hinaus dürfen Endnutzer:innen berechtigterweise die Erwartung haben, dass sie einfach untätig bleiben können, wenn sie nicht einwilligen möchten. In Fällen, in denen es nicht möglich ist, untätig zu bleiben, weil ein Einwilligungsbanner den Zugriff auf einige oder alle Inhalte des digitalen Angebots versperrt, müssen Endnutzer:innen ihre Ablehnung zumindest ohne Mehraufwand an Klicks (gegenüber der Zustimmung) äußern können. Diese Wertung wird auch durch Erwägungsgrund 32 S. 6 der DS-GVO gestützt, der die Vorgaben zur Einwilligung präzisiert. Demnach muss die Aufforderung in klarer und knapper Form und ohne unnötige Unterbrechung des Dienstes, für den die Einwilligung gegeben wird, erfolgen, wenn die betroffene Person auf elektronischem Weg zur Einwilligung aufgefordert wird.

(49) Eine wirksame Einwilligung liegt zudem regelmäßig nicht vor, wenn Nutzenden nur zwei Handlungsmöglichkeiten zur Auswahl gestellt werden, die nicht gleich schnell zu dem Ziel führen, den digitalen Dienst nutzen zu können. Hierbei wird ihnen einerseits eine Schaltfläche zum „Alles Akzeptieren“ angezeigt, andererseits eine Schaltfläche mit Bezeichnungen wie „Einstellungen“, „Weitere Informationen“ oder „Details“. Mittels der ersten Schaltfläche können die Endnutzer:innen unmittelbar und ohne

[31] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, S. 22, Beispiel 16.

weiteren Aufwand eine zustimmende Willenserklärung abgeben und das Angebot sofort nutzen. Mit der anderen Schaltfläche können die Nutzenden weder ablehnen noch eine sonstige Willenserklärung abgeben, sondern lediglich weitere Handlungsschritte einleiten. Es bedarf dann weiterer Entscheidungen oder Einstellungen, bis das gewünschte Angebot genutzt werden kann. Diese beiden Handlungsoptionen haben somit nicht denselben Kommunikationseffekt. Wenn Nutzende in dieser Konstellation die einzig vorhandene Schaltfläche wählen, mit der unmittelbar eine – den Entscheidungsprozess beendende – Willenserklärung abgeben werden kann, so kann dieser Handlung auch der Wille innewohnen, sich mit der Angelegenheit einfach nicht mehr beschäftigen zu müssen. Dies gilt umso mehr, wenn aufgrund der konkreten Beschriftung der Schaltflächen nicht einmal eindeutig zu erkennen ist, wie viel Mehraufwand erforderlich ist, um eine Ablehnung mitzuteilen.

(50) Um nachweisen zu können, dass Endnutzer:innen eine unmissverständliche und eindeutig bestätigende Handlung abgegeben haben, müssen diesen also mindestens solche Auswahloptionen angeboten werden, deren Kommunikationseffekt gleichwertig ist. Ist eine Auswahloption präzise dargestellt und erzeugt unmittelbar einen Effekt (z. B. eine „Alles Akzeptieren“-Schaltfläche), während die andere Option nebulös gehalten wird und nicht ermöglicht, den wahren gegenteiligen Willen mit demselben Aufwand zu äußern, besteht ein Effekt- und Informationsdefizit. Ein solches Defizit ist geeignet, Endnutzer:innen dazu zu bewegen, ihre Entscheidung nicht nach dem eindeutigen Willen, sondern nur danach zu treffen, welche Option die Einwilligungsabfrage eindeutig schneller beendet. Werden den Nutzenden keine gleichwertigen Handlungsmöglichkeiten offeriert, um die Einwilligung zu erteilen oder sie abzulehnen, so liegen die Anforderungen an eine wirksame Einwilligung regelmäßig nicht vor.[32]

e) Bezogen auf den bestimmten Fall

(51) Darüber hinaus muss die Einwilligung für den bestimmten Fall eingeholt werden. Es ist mithin nicht möglich, eine Generaleinwilligung oder Blankoeinwilligung für den generellen Einsatz bestimmter Techniken, z. B. Cookies, oder für diverse potentielle Folgeverarbeitungen einzuholen. Das Bestimmtheitserfordernis ist eng mit dem Merkmal „in informierter Weise“ verbunden und überschneidet sich auch mit den Kriterien, ob eine Einwilligung freiwillig erteilt wurde. Bevor eine Einwilligung abgefragt wird, muss ein eindeutiger und legitimer Zweck für die beabsichtigten Prozesse festgelegt werden, um die Endnutzer:innen sodann ausreichend hierüber informieren zu können. Bereits die Art. 29-Datenschutzgruppe als Vorgänger des Europäischen Datenschutzausschusses hat darauf hingewiesen, dass das Bestimmtheitserfordernis nicht durch vage oder allgemeine Angaben wie „Verbesserung der Erfahrungen des Nutzers“, „Werbezwecke“, „IT- Sicherheitszwecke“ oder „zukünftige Forschung“ erfüllt werden kann.[33]

---

[32] Einige Anbieter:innen von digitalen Diensten stellen Nutzende vor die Wahl, alternativ zur Erteilung einer Einwilligung ein kostenpflichtiges Abonnement abzuschließen. Diese spezielle Konstellation ist nicht Gegenstand der vorangehenden Ausführungen und Bewertung. Zu den rechtlichen Besonderheiten solcher Pur-Abo-Modelle auf Websites hat die DSK jedoch am 22. März 2023 einen Beschluss veröffentlicht, der abrufbar ist unter www.datenschutzkonferenz-online.de/media/pm/DSK_Beschluss_Bewertung_von_Pur-Abo-Modellen_auf_Websites.pdf.

[33] Art. 29-Datenschutzgruppe, Stellungnahme 03/2013 zur Zweckbindung (WP 203), S. 16.

(52) An dieser Anforderung hat sich auch durch die DS-GVO nichts geändert.[34] Nur wenn den Endnutzer:innen ausreichende Informationen über alle Zwecke zur Verfügung stehen, zu denen auf die Endeinrichtung zugegriffen werden soll, können diese überhaupt nachvollziehen, für welche Fälle sie ihre Einwilligung erteilen. Unabhängig davon, ob so dann die Möglichkeit besteht, über eine Handlung in alle Zwecke einzuwilligen oder diese abzulehnen, müssen Endnutzer:innen sodann auch separat einwilligen oder diese ablehnen können. Fehlt es an der nötigen Granularität, hat dies auch noch weitere Auswirkungen auf die Freiwilligkeit und damit die Wirksamkeit der Einwilligung. Denn Erwägungsgrund 43 der DS-GVO bringt deutlich zum Ausdruck, dass die Einwilligung regelmäßig auch dann nicht als freiwillig erteilt gilt, wenn zu verschiedenen Vorgängen nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies in dem entsprechenden Fall angemessen wäre. Eine Bündelung von Zwecken kann nur in Betracht kommen, wenn die Zwecke in einem sehr engen Zusammenhang stehen.[35]

(53) Grundsätzlich ist es möglich, Einwilligungsbannner mehrschichtig zu gestalten, also detailliertere Informationen erst auf einer zweiten Ebene des Banners mitzuteilen, zu der die Nutzenden über einen Button oder Link gelangen. Wenn jedoch bereits auf der ersten Ebene des Banners ein Button existiert, mit dem eine Einwilligung für verschiedene Zwecke erteilt werden kann, müssen auch auf dieser ersten Ebene konkrete Informationen zu allen einzelnen Zwecken enthalten sein. Zu unbestimmt wäre es, hier lediglich generische, allgemeine oder vage Informationen zu den Zwecken anzugeben, wie z. B. „Um Ihnen ein besseres Nutzungserlebnis bieten zu können, verwenden wir Cookies“.

f) Freiwilligkeit der Einwilligung

(54) Schließlich ist die Einwilligung nur wirksam, wenn die Willensbekundung freiwillig erfolgt ist. Hierzu heißt es in den Leitlinien 05/2020 des Europäischen Datenschutzausschusses zur Einwilligung:

> *„Das Element „frei“ impliziert, dass die betroffenen Personen eine echte Wahl und die Kontrolle haben. Im Allgemeinen schreibt die DSGVO vor, dass eine Einwilligung nicht gültig ist, wenn die betroffene Person keine wirkliche Wahl hat, sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt. […] Entsprechend wird eine Einwilligung nicht als freiwillig angesehen, wenn die betroffene Person die Einwilligung nicht verweigern oder zurückziehen kann, ohne Nachteile zu erleiden. In der DSGVO wird auch das Konzept des „Ungleichgewichts“ zwischen dem Verantwortlichen und der betroffenen Person berücksichtigt.*
>
> *Grundsätzlich wird eine Einwilligung durch jede Form des unangemessenen Drucks oder der Einflussnahme (die sich auf viele verschiedene Weisen manifestieren können) auf die betroffene Person, die diese von der Ausübung ihres freien Willens abhalten, unwirksam*.“[36]

(55) Gemäß Erwägungsgrund 42 Satz 5 DS-GVO sollte davon ausgegangen werden, dass die betroffene Person ihre Einwilligung nur dann freiwillig gegeben hat, wenn sie eine echte und freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden. Auch ist zu berücksichtigen, ob unter anderem die Erfüllung eines Vertrages davon abhängig gemacht wird,

---

[34] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 55.
[35] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 43.
[36] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 13 und 14.

dass in eine Datenverarbeitung eingewilligt wird, die für die Vertragserfüllung nicht erforderlich ist. Eine solche Koppelung führt gemäß Art. 7 Abs. 4 DS-GVO regelmäßig dazu, dass die Einwilligung nicht als freiwillig angesehen werden kann und damit unwirksam ist.[37]

(56) Bei der Bewertung, ob die Einwilligung für den Zugriff auf Endgeräte des Endnutzers freiwillig erteilt wurde, ist zunächst zu klären, ob überhaupt ein Zwang für die Endnutzer:innen bestand, eine Erklärung abzugeben, oder ob sie untätig hätten bleiben können. Es ist davon auszugehen, dass ein solcher Zwang besteht, wenn ein Banner oder sonstiges grafisches Element zur Einwilligungsabfrage den Zugriff auf die Webseite insgesamt oder Teile des Inhalts verdeckt und das Banner nicht einfach ohne Entscheidung geschlossen werden kann.[38]

(57) Zwar gehen Stimmen in der Literatur davon aus, dass niemand gezwungen sei, eine Webseite zu besuchen, deren Inhalt grundsätzlich auch von anderen am Markt angeboten wird. Diese Argumentation kann jedoch nicht durchgreifen. Wie bereits der Europäische Datenschutzausschuss (sowie dessen Vorgängerinstitution) verdeutlicht hat, kann eine Einwilligung nicht deshalb als freiwillig erteilt angesehen werden, weil zwischen einer Dienstleistung, zu der die Einwilligung in die Nutzung personenbezogener Daten für zusätzliche Zwecke gehört, und einer vergleichbaren Dienstleistung, die von einem anderen Verantwortlichen angeboten wird, eine Wahlmöglichkeit besteht.[39] In einem solchen Fall wäre die Wahlmöglichkeit vom Verhalten anderer Marktteilnehmer und davon abhängig, ob eine betroffene Einzelperson die Dienstleistungen des anderen Verantwortlichen wirklich als gleichwertig ansehen würde. Dies würde darüber hinaus bedeuten, dass der Verantwortliche die Entwicklungen des Marktes verfolgen müsste, um eine fortgesetzte Gültigkeit der Einwilligung in die Datenverarbeitungstätigkeiten sicherzustellen, da ein Wettbewerber seine Dienstleistungen zu einem späteren Zeitpunkt ändern könnte. Daher kann eine Einwilligung nicht per se nur deshalb als freiwillig qualifiziert werden, wenn Betroffene sich theoretisch alternativen Optionen hätte zuwenden können, die ein Dritter anbietet. Diese Argumentation, die zu Datenverarbeitungsprozessen getroffen wurde, ist auf den Zugriff auf Endeinrichtungen übertragbar, da auch insoweit die Anforderungen der DS-GVO gelten.

(58) Das Merkmal der Freiwilligkeit wird auch dann spürbar beeinflusst, wenn die Ablehnung aller einwilligungsbedürftigen Zugriffe einen messbaren Mehraufwand für Endnutzer:innen bedeutet. Ein solcher Mehraufwand wird z. B. erzeugt, indem die Ablehnung erst auf einer zweiten Banner-Ebene, und damit nur mit einer höheren Anzahl an Klicks möglich ist (im Vergleich zur Zustimmung). Der Mehraufwand besteht in der Regel auch nicht lediglich darin, dass Endnutzer:innen einmal mehr klicken müssen als bei der Zustimmung. Sie müssen vielmehr darüber hinaus auch die weiteren Informationen und Einstellungsmöglichkeiten, mit denen sie auf einer zweiten Ebene der Einwilligungsdialoge konfrontiert werden, lesen, nachvollziehen und dann unter den weiteren Auswahloptionen die zutreffende auswählen. Der erzeugte Mehraufwand lässt sich grundsätzlich auch nicht sachlich begründen (z. B. mit technischen Hindernissen), sondern wird künstlich konstruiert. Dies lässt sich nicht zuletzt daraus schließen, dass Endnutzer:innen mittlerweile auf einer Vielzahl an Webseiten durchaus eine gleich einfache Ablehnungsmöglichkeit zur Auswahl gestellt wird.

---

[37] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 14.

[38] Zu den hiervon zu unterscheidenden Cookie-Walls siehe EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 39-41.

[39] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 38.

(59) Wenn Nutzende beim Aufruf eines digitalen Dienstes eine Einwilligungsabfrage nicht einfach ignorieren können, weil diese Inhalte des Angebots verdeckt, fehlt es somit regelmäßig an der Freiwilligkeit der Einwilligung, wenn die Erteilung der Ablehnung mit einem höheren Aufwand, z. B. an Klicks und Aufmerksamkeit, verbunden ist. Um sicherzustellen, dass sie eine wirksame Einwilligung nachweisen können, müssen Anbieter:innen von digitalen Diensten daher dringend darauf achten, die zur Auswahl gestellten Optionen gleichwertig zu gestalten.

(60) In die Bewertung ist an dieser Stelle auch der Grundsatz von Treu und Glauben gemäß Art. 5 Abs. 1 lit. a) DS-GVO einzubeziehen. Kann kein sachlicher Grund dafür vorgebracht werden, warum z. B. keine mit demselben Aufwand verbundene Ablehnungsmöglichkeit auf erster Ebene eines Cookie-Banners angeboten wird, stellt dies einen Versuch dar, in treuwidriger Weise Einfluss auf die Endnutzer:innen zu nehmen. Im Zusammenhang mit Telefonwerbung hat der Bundesgerichtshof entschieden, dass eine Einwilligung jedenfalls dann unwirksam ist, wenn die Gestaltung darauf angelegt ist, die Betroffenen von der Ausübung ihres Wahlrechts abzuhalten.[40]

g) Möglichkeit zum Widerruf der Einwilligung

(61) Aus Art. 7 Abs. 3 Satz 4 DS-GVO ergibt sich, dass der Widerruf einer Einwilligung ebenso einfach möglich sein muss wie die Erteilung.

(62) Wird die Einwilligung unmittelbar bei der Nutzung einer Webseite erteilt, muss auch deren Widerruf auf diesem Weg möglich sein. Nicht den Vorgaben entsprechen ausschließliche Widerrufsmöglichkeiten über andere Kommunikationswege wie E-Mail, Fax oder sogar per Brief. Es ist auch unzulässig, Nutzende auf ein Kontaktformular hinzuweisen, da in diesem Fall zwar derselbe Kommunikationsweg (d. h. über die Webseite) verwendet wird, aber die Anforderungen deutlich höher sind als bei der Erteilung der Einwilligung (und mittels Kontaktformular Daten erhoben würden, die für den Widerruf nicht erforderlich sind). Wurde eine Einwilligung mittels Banner o. Ä. abgefragt, ist es daher auch unzulässig, wenn zunächst eine Datenschutzerklärung aufgerufen und dann in dieser zu der richtigen Stelle gescrollt werden muss, um zu einer Widerrufsmöglichkeit zu gelangen. Ein solcher Suchvorgang als Zwischenschritt wäre eine Erschwerung, die mit den gesetzlichen Vorgaben nicht vereinbar ist. Dieser Umweg ist auch nicht auf eine technische Unmöglichkeit zurückzuführen, da eine Vielzahl an Webseiten einen stets sichtbaren Direktlink oder ein Icon anzeigen, das unmittelbar zu den relevanten Einstellungsmöglichkeiten führt. Es genügt den gesetzlichen Anforderungen erst recht nicht, wenn an verschiedenen Stellen der Datenschutzerklärung auf Opt-out Möglichkeiten auf unterschiedlichen externen Webseiten hingewiesen wird. Gleichwohl bedeutet dies nicht, dass der Widerruf über einen Verweis in einer Datenschutzerklärung per se abzulehnen ist. Sofern Verlinkungen die Nutzenden direkt an die Stelle zur Möglichkeit des Widerrufs leiten und gerade keine Suchvorgänge nötig sind, kann eine direkt auffindbare Widerrufsmöglichkeit auch in einer Datenschutzerklärung platziert werden.

h) Gültigkeit der Einwilligung

(63) „Die DS-GVO enthält keine spezifischen Vorgaben zur Dauer der Wirksamkeit einer Einwilligung. Wie lange die Einwilligung gültig ist, hängt vom Kontext, dem Umfang der ursprünglichen Einwilligung und

[40] BGH, Urteil vom 28. Mai 2020 – I ZR 7/16 Rn. 37 – Cookie-Einwilligung II (Planet49).

den Erwartungen der betroffenen Partei ab."[41] Zu beachten ist, dass sich Einwilligungen immer auf „den bestimmten Fall" beziehen. Ändert sich der „Fall" wird die ursprüngliche Einwilligung gegenstandslos und es ist eine neue Einwilligung einzuholen. Wird durch eine bestätigende Handlung eine gebündelte Einwilligung für zahlreiche Fälle eingeholt, wie dies regelmäßig auf Webseiten und in Apps erfolgt, führt jede Änderung insbesondere der eingesetzten Cookies und eingebundenen Drittdienste dazu, dass für den neuen Fall eine neue Einwilligung eingeholt werden muss. Wird diese nicht einzeln abgefragt, muss die gebündelte Einwilligung erneut eingeholt werden.

3. Ausnahmen von der Einwilligungsbedürftigkeit

(64) Von dem Grundsatz der Einwilligungsbedürftigkeit sind in § 25 Abs. 2 TDDDG zwei Ausnahmen vorgesehen. Die erste Ausnahme richtet sich vornehmlich an Anbieter von Telekommunikationsdiensten i.S.v. § 3 Nr. 1 TKG n.F. Die zweite Ausnahme adressiert im Unterschied dazu die Anbieter:innen von digitalen Diensten gemäß § 2 Abs. 2 Nr. 1 TDDDG.

a) Durchführung der Übertragung einer Nachricht

(65) Gemäß § 25 Abs. 2 Nr. 1 TDDDG ist eine Einwilligung nicht erforderlich, wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung der Nutzenden gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist.

b) Zurverfügungstellen eines digitalen Dienstes

(66) § 25 Abs. 2 Nr. 2 TDDDG fordert keine Einwilligung, wenn die Speicherung von Informationen in der Endeinrichtung oder der Zugriff auf bereits in der Endeinrichtung gespeicherte Informationen unbedingt erforderlich ist, damit Anbieter:innen eines digitalen Dienstes einen von der/dem jeweiligen Nutzenden ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen können.

(67) Im Gesetzgebungsverfahren zum TDDDG und auch in dem europäischen Verfahren zum Erlass der e-Privacy-Verordnung wurde und wird deutlich, dass es viele Bestrebungen gibt, deutlich mehr Ausnahmen vom Einwilligungserfordernis zuzulassen, als dies aktuell in Art. 5 Abs. 3 S. 2 ePrivacy-RL vorgesehen ist. Dennoch hat sich der deutsche Gesetzgeber entschieden, § 25 Abs. 2 TDDDG sehr eng am Wortlaut der europäischen Vorschrift anzulehnen und keine über Art. 5 Abs. 3 S. 2 ePrivacy-RL hinausgehenden Ausnahmen aufzunehmen. Die Vorschrift enthält im Wesentlichen zwei Tatbestandsmerkmale, die grundsätzlich auslegungsbedürftig sind – dies sind „einen vom Nutzer ausdrücklich gewünschten digitalen Dienst" und „unbedingt erforderlich". Beide Tatbestandsmerkmale stehen in einem untrennbaren Zusammenhang. Die unbedingte Erforderlichkeit von Speicher- und Auslesevorgängen ist in Bezug auf den konkret von der Endnutzerin oder dem Endnutzer gewünschten digitalen Dienst zu prüfen, um festzustellen, ob die Ausnahmevorschrift greift.

(68) Bei der Prüfung der Voraussetzungen ist zu beachten, dass § 25 TDDDG eine andere Systematik aufweist als Art. 6 Abs. 1 DS-GVO. § 25 TDDDG sieht nur zwei Legitimationsmöglichkeiten vor. Entweder liegt eine wirksame Einwilligung der Endnutzer:innen vor oder es sind die Voraussetzungen einer der

[41] EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 110.

beiden in Absatz 2 geregelten Ausnahmen erfüllt. Art. 6 Abs. 1 DS-GVO sieht demgegenüber mehrere Möglichkeiten für die rechtmäßige Verarbeitung personenbezogener Daten vor, von denen die Einwilligung gemäß Art. 6 Abs. 1 lit. a) DS-GVO nur eine von mehreren gleichrangigen Varianten ist.

(69) Die Ausnahmen gemäß § 25 Abs. 2 TDDDG unterscheiden sich zudem wesentlich von Art. 6 Abs. 1 lit. f) DS-GVO, der bis zum 30. November 2021 von den Aufsichtsbehörden unter engen Voraussetzungen als mögliche Rechtsgrundlage angesehen worden ist. Während das TDDDG starre Kriterien benennt, die erfüllt sein müssen, eröffnet die DS-GVO eine gewisse Abwägungsflexibilität. Keinesfalls ist eine Interessenabwägung, die zu Art. 6 Abs. 1 lit. f) DS-GVO vorgenommen wurde, geeignet, automatisch die Voraussetzungen von § 25 Abs. 2 Nr. 2 TDDDG zu begründen. Zur Umsetzung der neuen Rechtslage ist es daher nicht ausreichend, wenn lediglich die Bezeichnung der Rechtsgrundlagen in einer Datenschutzerklärung ausgetauscht wird.

aa. Von Endnutzer:innen ausdrücklich gewünschter digitaler Dienst

(70) Die Bewertung, ob die Inanspruchnahme eines digitalen Dienstes ausdrücklich von Endnutzer:innen gewünscht ist, erfordert im Ergebnis, eine innere, persönliche Einstellung festzustellen. Diese kann nur aus objektiven Kriterien, wie insbesondere den Handlungen der Nutzenden abgeleitet werden. Im Kontext von Webseiten und Apps nehmen Nutzende einen digitalen Dienst grundsätzlich in Anspruch, indem sie ihn bewusst aufrufen.[42] Dies erfolgt regelmäßig durch die Eingabe der URL der Webseite in einem Browser, durch das Anklicken eines Links auf einer zuvor erfolgten Suche in einer Suchmaschine oder die Installation einer App. Diese eine Handlung lässt allerdings nicht den Schluss zu, dass das hinter der URL oder App verborgene oder über den Link angesprochen gesamte Webseitenangebot, ggf. inklusive diverser Unterseiten ausdrücklich gewünscht ist.

(71) Weitaus seltener kommt es in der Praxis vor, dass digitale Dienste auf der Grundlage eines zuvor geschlossenen Vertrags genutzt werden. Dies ist insbesondere bei zahlungspflichtigen Diensten, wie z.B. Beck Online, anzunehmen. Liegen ein (schriftlicher) Vertrag über die Nutzung des digitalen Dienstes oder ergänzende Nutzungsbedingungen, aus denen der konkrete Leistungsumfang entnommen werden kann, vor, können diese Dokumente zur Bestimmung des Nutzerwunsches herangezogen werden.

(72) Es ist entscheidend, welches Verständnis dem Begriff „digitaler Dienst“ im Zusammenhang mit § 25 Abs. 2 Nr. 2 TDDDG zugrunde liegt. Dieser lässt sich einerseits global, also z. B. einer Webseite insgesamt, als auch granular, z. B. nur eine bestimmte Funktion oder bestimmte Inhalte einer Webseite, interpretieren. Die Webseite eines Unternehmens kann z. B. Informationen über das Unternehmen, einen Online-Shop, Kontaktmöglichkeiten via Kontaktformular, einen eingebundenen Chat, einen Routenplaner zum Unternehmen sowie Eigen- und Drittwerbung beinhalten.

(73) Allgemein auf einen gesamten digitalen Dienst, ggf. inklusive diverser Unterseiten, abzustellen, ist insbesondere in Bezug auf hochkomplex gestaltete Webseiten und Apps regelmäßig nicht der richtige Maßstab. Der durch § 25 TDDDG umgesetzte Art. 5 Abs. 3 ePrivacy-RL stellt auf „einen vom Teilnehmer

[42] Werden bei der Nutzung eines digitalen Dienstes Informationen im vernetzten Fahrzeug oder Smarthome-Geräten gespeichert oder auf diese zugegriffen, z. B im Rahmen des Entertainmentsystems von Fahrzeugen oder einer App zum Abschließen des Fahrzeugs, ist an vergleichbare Handlungen des Nutzers anzuknüpfen. In Bezug auf vernetzte Fahrzeuge s. auch EDSA, Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, Rn. 10 ff. und beispielhaft für Smarthome-Geräte die EDSA Leitlinien 02/2021 zu virtuellen Sprachassistenten Version 2.0, Rn. 28 ff.

oder Nutzer ausdrücklich gewünschten Dienst der Informationsgesellschaft“ ab. Bei vielen Angeboten wird nicht „ein“ Dienst, sondern ein Bündel von Dienstleistungen mit verschiedenen Funktionen angeboten, die bei einem Besuch durch die einzelnen Nutzer:innen kaum immer alle genutzt werden. Diese Dienstleistungen werden gerade für die Adressaten der Webseiten oder Apps erbracht und nicht als reiner Selbstzweck. Gleichzeitig verfolgen Anbieter:innen der Webseiten oder Apps oder eingebundene Drittdienstleister darüber hinausgehende eigene Interessen. Die differenzierte Betrachtung einer Webseite oder App entspricht dem Zweck der Norm, nur diejenigen Eingriffe in die Endgeräte der Nutzer:innen zu erlauben, die im konkreten Fall unbedingt erforderlich sind, weil ohne sie der konkret vom einzelnen Nutzenden gewünschte Dienst nicht erbracht werden kann. Würde man auf eine Webseite oder App als Ganzes abstellen, hätten es Anbieter:innen von digitalen Diensten in der Hand, durch umfassende Einbettung diverser in der Praxis nicht genutzter, aber mit unter Umständen sehr invasiven Datenverarbeitungen verbundener Funktionen den Umfang des digitalen Dienstes beliebig zu bestimmen. Der Wunsch der Nutzenden bliebe bei einer globalen Interpretation unbeachtet. Entsprechend hatte sich bereits die Art. 29-Datenschutzgruppe zur ePrivacy-RL für eine solche granulare Betrachtung des Dienstes ausgesprochen. Demnach sei ein Dienst als Summe verschiedener Funktionen zu betrachten und könne daher abhängig von den von Nutzer:innen aufgerufenen Funktionen einen unterschiedlichen Umfang aufweisen.[43]

(74) Es ist daher zunächst zu bestimmen, welcher Nutzerwunsch aus dem Aufruf der Webseite oder der App geschlossen werden kann.[44] Jeder digitale Dienst weist einen Basisdienst auf, der untrennbar für das gesamte Angebot von Bedeutung ist. Die Basisdienste lassen sich regelmäßig aus der Kategorie des digitalen Dienstes ableiten. Als beispielhafte Kategorien seien hier Webshops, Suchmaschinen, Informationsseiten von Unternehmen oder öffentlichen Einrichtungen, Behördenportale, Online-Banking, Blogs, Soziale Netzwerke und Übersetzungsdienste genannt. Basisdienst eines Webshops ist der Verkauf von Produkten. Basisdienst einer Suchmaschine ist, dass bei Eingabe eines Suchbegriffs passende Webseiten im Internet gefunden und über Hyperlinks als Suchergebnisse aufgelistet werden. Der Basisdienst wird oft von Komponenten flankiert, damit dieser sicher, schnell und stabil zur Verfügung gestellt werden kann. Solche Systeme zur nutzerorientierten Betrugsprävention und IT-Sicherheit dienen grundsätzlich gleichermaßen den Nutzer:innen und dem Betreiber der Webseite und können dem Basisdienst zugerechnet werden. Für bestimmte Kategorien von digitalen Diensten gibt es weitere nutzerorientierte Zusatzfunktionen, durch die der Basisdienst unterstützt wird, wie beispielsweise die Einkaufskorbfunktion bei Online-Shops. Die Zusatzfunktionen sind in den Basisdienst integriert, kommen jedoch für manche Nutzer:innen gar nicht oder nicht über den gesamten Zeitraum der Nutzung des Angebots zum Tragen. Neben diesen Basisdiensten werden Nutzer:innen häufig Zusatzdienste und Funktionen zur Verfügung gestellt, die grundsätzlich unabhängig von der Kategorie des digitalen Dienstes sind, wie z. B. Spracheinstellungen, Chatboxen, Kontaktformulare, Push-Nachrichten, Kartendienste, Wetterdienste, Videos und Audios, Log-in Bereiche inkl. Authentifizierung, Werbung, Verwaltung von Einwilligungen mittels Consent-Management-Tools, Merklisten oder Favoritenlisten.

---

[43] Vgl. Art. 29-Datenschutzgruppe, Stellungnahme 4/2012 zur Ausnahme von Cookies von der Einwilligungspflicht (WP 194), S. 4.

[44] Wie der Nutzerwunsch sodann realisiert wird, ist in einem weiteren Schritt zu beurteilen, siehe sogleich unter bb. Unbedingt erforderlich.

(75) Zwar besteht zumindest im privatrechtlichen Kontext grundsätzlich eine Gestaltungsfreiheit der Anbieter:innen der digitalen Dienste. Mit welchen Funktionalitäten Anbieter:innen, z. B. einen Online-Shop, eine News-Seite, ein Bewertungsportal oder ein soziales Netzwerk ausstatten, steht ihnen daher grundsätzlich frei. Jedoch stellt § 25 Abs. 2 Nr. 2 TDDDG aufgrund der Formulierung „vom Nutzer ausdrücklich gewünschten digitalen Dienst“ explizit auf die Perspektive der Nutzer:innen ab, die mithin maßgeblich mit einzubeziehen ist.

(76) Der Basisdienst ist grundsätzlich als der von Nutzer:innen gewünschte digitale Dienst anzusehen, sobald diese einen Dienst bewusst aufrufen. Aus dieser Handlung kann allerdings nicht automatisch der Schluss gezogen werden, dass der Nutzende alle Zusatzfunktionen des Basisdienstes wünscht. Welcher Funktionsumfang gewünscht ist, ist im Einzelfall aus der Perspektive durchschnittlich verständiger Nutzer:innen zu beurteilen. Der Basisdienst von Webshops weist z. B. eine Warenkorbfunktion und integrierte Zahlfunktionen auf. Diese sind allerdings erst dann von Nutzenden gewünscht, wenn tatsächlich ein Produkt in den Warenkorb gelegt oder eine Zahlfunktion ausgewählt wird. Zusatzdienste und -funktionen, die unabhängig vom Basisdienst individuell in Anspruch genommen werden können, wie z. B. ein Kontaktformular, ein Chat oder ein Kartendienst, werden ebenfalls nicht automatisch mit dem ersten Aufruf der Webseite oder App von Nutzer:innen gewünscht. Häufig haben Nutzende vor dem Aufruf des Angebots gar keine weitergehenden Kenntnisse über den genauen Dienstleistungs- und Funktionsumfang der Webseite oder App. Nutzer:innen „wünschen“ die beispielhaft genannten Zusatzdienste und -funktionen erst, wenn sie diese explizit in Anspruch nehmen, z. B. einen Chatbot anklicken, eine Merkliste anlegen oder ein Formular ausfüllen. Der ausdrückliche Wunsch der Nutzenden in Bezug auf diese Zusatzdienste und -funktionen muss sich daher in weiteren Handlungen ausdrücken. Dies bedeutet im Webseitenkontext, dass Nutzer:innen nicht jeden Zugriff auf ihre Endeinrichtung, insbesondere das Setzen von Cookies hinnehmen müssen, nur weil eine Webseite oder eine App aktiv aufgerufen wurde. Nutzer:innen müssen zunächst Kenntnis darüber erlangen (können), dass es Zusatzdienste und -funktionen gibt, zu deren Bereitstellung ein Zugriff auf die Endeinrichtung erforderlich ist, und eine Zusatzfunktion bewusst nutzen.

(77) Schließlich können auf Webseiten oder Apps zusätzliche allgemeine Funktionen integriert sein, wie beispielsweise die Messung und/oder Analyse von Besucherzahlen oder A/B-Tests. Diese sind nicht per se dem Basisdienst zuzurechnen. Die Nutzer:innen können diese regelmäßig aber auch nicht bewusst wahrnehmen und daher nicht aktiv auswählen. Hier kommt es für die Bewertung darauf an, ob die konkreten, sehr differenziert zu betrachtenden Zwecke der Funktionen nutzerorientiert erfolgen.

Die dargestellte Aufspaltung in Basisdienst und Zusatzfunktionen dient als Hilfestellung für die vorzunehmende granulare Betrachtung des digitalen Dienstes, an der sich Anbieter:innen von digitalen Diensten orientieren können. Sie ermöglicht eine systematische und nachvollziehbare Prüfung, welche Bestandteile eines digitalen Dienstes aufgrund welcher Handlung des Nutzers gegebenenfalls zu unterschiedlichen Zeitpunkten der Nutzung einer Webseite als von ihm ausdrücklich gewünscht einzustufen sind. Gleichzeitig wird der Prüfungsmaßstab der Aufsichtsbehörden hierdurch transparent dargelegt.

bb. Unbedingt erforderlich

(78) Das Merkmal „unbedingt erforderlich“ wird weder im TDDDG noch in der ePrivacy-RL näher definiert. In der Gesetzesbegründung zum TDDDG wird jedoch von einer technischen Erforderlichkeit ausgegangen, was ein strenges Verständnis nahelegt.[45] Dies bedeutet, dass auch für von Endnutzer:innen ausdrücklich gewünschte Dienste nur solche Zugriffe auf die Endeinrichtung von der Ausnahme umfasst sind, die technisch erforderlich sind, um gerade den gewünschten Dienst bereitzustellen.[46] Denn das Kriterium der Erforderlichkeit im Sinne der Vorschrift bezieht sich ausschließlich auf die Funktionalität des digitalen Dienstes als solchen. Eine Ausnahme von der Einwilligungsbedürftigkeit kann daher nicht dadurch begründet werden, dass das Speichern von oder der Zugriff auf Informationen im Endgerät wirtschaftlich für das Geschäftsmodell erforderlich ist, in das der digitale Dienst eingebunden ist.

(79) Neben der Frage des „Ob“ hat das Kriterium der unbedingten Erforderlichkeit noch zeitliche, inhaltliche und personelle Dimensionen. In den Blick zu nehmen sind stets der Zeitpunkt der Speicherung (Wann?) und die Laufzeit des Cookies (Wie lange?), der Inhalt des Cookies (Was?) sowie die setzende Domäne eines Cookies, die darüber entscheidet, wer die Informationen auslesen kann (Für wen?). Der Zugriff auf die Endeinrichtung und der Zugriff auf die Informationen im Sinne der Norm sind hinsichtlich aller Dimensionen auf das erforderliche Minimum zu reduzieren.

(80) Cookies für etwaige Zusatzfunktionen, z. B. zur Speicherung von Produkten im Warenkorb oder Durchführung einer Zahlung, können in Bezug auf die zeitliche Dimension regelmäßig erst dann als unbedingt erforderlich betrachtet werden, wenn eine entsprechende Nutzerinteraktion stattgefunden hat, also tatsächlich ein Artikel in den Warenkorb gelegt oder der Zahlprozess eingeleitet wurde. Für eine bloße Nutzung des Angebots, also z. B. das Stöbern in einem Webshop, ist es nicht erforderlich, dass die Warenkorb- und Zahlungsfunktionen bereits aktiviert sind. Auch wird bei individualisierten Cookies die Gültigkeit häufig nur für eine Session erforderlich sein. Gemäß § 19 Abs. 1 TDDDG ist grundsätzlich davon auszugehen, dass unter der Nutzung eines digitalen Dienstes ein einzelner Nutzungsvorgang zu verstehen ist, also eine Session.[47] Eine regelmäßige Nutzung des digitalen Dienstes durch bestimmte Endnutzer:innen kann grundsätzlich nur dann unterstellt werden, wenn es sich um einen anmeldepflichtigen Dienst handelt.

(81) Ausgehend vom Zweck des § 25 TDDDG, die Privatsphäre bei Endeinrichtungen zu schützen, sind bei der inhaltlichen Dimension vor allem Prozesse zu hinterfragen, bei denen eindeutige Identifikations-Kennzeichnungen (Cookie-UIDs) vergeben werden, weil insbesondere diese Eingriffe in die Privatsphäre zur Folge haben. Für derartige Speicherungen besteht nur in wenigen Fällen eine unbedingte Erforderlichkeit, da viele Funktionen, die mittels der Speicherung von Informationen auf und dem Auslesen dieser von Endgeräten der Nutzenden umgesetzt werden sollen, ohne Individualisierung erfolgen können. So ist es beispielsweise nicht als erforderlich zu betrachten, dass für die Speicherung einer Einwilligung oder für Load-Balancing ein Cookie mit einer eindeutigen ID langfristig gespeichert wird

---

[45] BT-Drs. 19/27441 S. 38, siehe auch DSB, FAQ zum Thema Cookies und Datenschutz, Stand 20.12.2023, abrufbar unter https://www.dsb.gv.at/download-links/FAQ-zum-Thema-Cookies-und-Datenschutz.html.

[46] Siehe hierzu auch Erwägungsgrund 66 der ePrivacy-RL: „Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen”.

[47] Ein Nutzungsvorgang ist im Kontext von Webseiten üblicherweise dann beendet, wenn Nutzende die Webseite oder den Browser aktiv schließen.

und abgerufen werden kann. Gleiches gilt für das Speichern von Einstellungen zur Sprache oder Hintergrund-Farbe. Hierfür ist kein ein eindeutiges Identifizierungsmerkmal wie eine eindeutige User-ID erforderlich, sondern es reicht die Speicherung einer jeweils nicht identifizierenden Angabe wie z. B. „background-color: black“ oder „language: de“.

(82) Auch die Frage, wer auf die Informationen zugreifen kann, ist mit Blick auf das Erforderlichkeitskriterium streng zu prüfen.

(83) Cookies die als unbedingt erforderlich eingeordnet werden können, hingegen sind nutzerorientierte Sicherheitscookies. Diese werden bspw. verwendet, um wiederholt fehlgeschlagene Anmeldeversuche auf einer Website zu entdecken. Umfasst werden auch andere ähnliche Mechanismen, die das Login-System vor Missbrauch schützen sollen. Beim Einsatz derartiger Cookies ist zu beachten, dass diese Ausnahmeregelung nur dann greift, wenn die hier dargestellten Voraussetzungen vorliegen. Eine pauschale Klassifizierung als „Sicherheitscookie“ ist nicht ausreichend. Weiterhin gilt dies nicht für Cookies, die der Sicherheit von Websites oder Diensten Dritter dienen, die nicht ausdrücklich vom Nutzer angefordert wurden.

(84) Im Zusammenhang mit der Speicherung von Einwilligungen, die von Nutzer:innen einer Webseite abgegeben werden, erfordert die Erfüllung der Nachweispflicht gemäß § 25 Abs. 1 S. 2 TDDDG i. V. m. Art. 7 Abs. 1 und Art. 5 Abs. 2 DS-GVO keine langlebigen UID-Cookies. In der Regel genügt es, nachzuweisen zu können, dass und welche Prozesse implementiert wurden, um eine Einwilligung einzuholen und das Ergebnis in einem Cookie ohne UID oder sonstige überschießende Informationen abzulegen.

(85) Die Darlegung der implementierten Prozesse umfasst nicht nur Informationen über die Einbindung eines Einwilligungsbanners oder einer CMP, sondern es sind weitere Informationen wie unter anderem auch Art und Weise der Speicherung und des Auslesens von Nutzer:innen-Entscheidungen, eine Beschreibung der einzelnen technischen Abläufe und die zum Zeitpunkt der erteilten Einwilligung vorgelegten Informationen erforderlich. Es sollten daher auch überholte Banner-Texte und -Konfigurationen gespeichert werden, um als Nachweis darauf zurückgreifen zu können.

(86) Zu beachten ist schließlich, dass es zwar möglich ist, zu verschiedenen Zwecken eine Information in einer Endeinrichtung zu speichern oder hierauf zuzugreifen, das heißt z. B. einen Cookie für verschiedene Zwecke zu verwenden. Doch kann ein solcher Mehrzweck-Cookie nur dann von der Einwilligungspflicht ausgenommen werden, wenn für jeden einzelnen Zweck, zu dem der Cookie verwendet wird, die Voraussetzungen der Ausnahme nach § 25 Abs. 2 Nr. 2 TDDDG vorliegen.[48]

c) Anwendungsbeispiele und Prüfkriterien

(87) Auf Webseiten und Apps werden zahlreiche Verfahren und Drittdienste eingesetzt, die in den Anwendungsbereich von § 25 TDDDG fallen und mit denen sehr unterschiedliche Zwecke verfolgt werden. Dabei haben sich mittlerweile einige Bezeichnungen und Formulierungen entwickelt, die regelmäßig verwendet werden um diese Dienste zu kategorisieren, wie z. B. Reichweitenmessung, Webseitenoptimierung, Betrugssicherheit und personalisierte Services. Aus Sicht der Verantwortlichen wäre es wünschenswert, wenn die Aufsichtsbehörden eine Aussage dazu treffen würden, ob beispielsweise

[48] S. Art. 29-Datenschutzgruppe, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht (WP 194), S. 6.

eine Reichweitenmessung gemäß § 25 Abs. 2 Nr. 2 TDDDG grundsätzlich ohne Einwilligung der Endnutzer:innen einer Webseiten eingesetzt werden darf. Aus mehreren Gründen finden sich in dieser Orientierungshilfe keine derartigen Aussagen. Dies wird nachfolgend am Beispiel der Reichweitenmessung verdeutlicht.

(88) Erstens sind die üblicherweise herangezogenen Bezeichnungen zu unbestimmt. Die Reichweitenmessung stammt ursprünglich aus dem Bereich der analogen Medien. Bei Pressemedien und Fernsehsendungen wird lediglich die Anzahl erfasst, wie viele Leser:innen, Zuschauer:innen und Zuhörer:innen das jeweilige Medienangebot erreicht hat. Bei Pressemedien und Büchern werden zunächst Verkaufszahlen ermittelt. Im Rundfunk und im Hinblick auf die Zahl der tatsächlichen Leser:innen gab es zumindest in der analogen Welt keine unmittelbare technische Möglichkeit, um zu ermitteln, welche Zuschauer:innen oder Zuhörer:innen welches Rundfunkprogramm eingeschaltet und welche Leser:innen welches Printmedium gelesen haben, so dass in einigen repräsentativen Haushalten Umfragen als Grundlage für die Berechnung von Einschaltquoten vorgenommen wurden. Übertragen auf den Webseitenkontext entsprechen Einschaltquoten einer reinen Zählung, wie häufig eine Webseite aufgerufen wird (page impression). Dafür reicht es aus, bei jedem Abruf einer Seite den Zähler für diese Seite um Eins zu erhöhen, auf der Basis von Logfiles ohne personenbezogene Daten die Zahl der jeweiligen Seitenabrufe zu ermitteln oder ein einfaches Zählpixel (des direkt aufgerufenen digitalen Dienstes) auf der Webseite zu implementieren, durch das keine weiteren Nutzerdaten erfasst werden. Angebote von Drittdienstleistern zur Reichweitenmessung auf Webseiten oder in Apps verarbeiten allerdings regelmäßig (teils sehr weitgehende) Informationen über Nutzende und stellen auf Basis dieser Informationen deutlich mehr Auswertungsergebnisse zur Verfügung. Die Auswertungen können grob unterschieden werden in Informationen über Besuchende, z. B. Geräte, Software, Zeiten, Benutzer-IDs und benutzerdefinierte Variablen, und Informationen über das Verhalten der Nutzenden auf der Webseite oder in der App, wie z. B. Einstiegs- und Ausstiegsseiten, Seitentitel, interne Suchen, Downloads und Eingaben. Diese Informationen werden zur Gewinnung weiterer Erkenntnisse verwendet, wie beispielsweise zur Analyse und Auswertung der durchschnittlichen Aufenthaltsdauer, Anzahl abgesprungener Besucher:innen, Aktionen pro Besuch, Seitenansichten, interne Suchen, Downloads oder auch auf welchem Weg die Nutzenden die Webseite aufgerufen haben.[49]

(89) Im Webseiten- und App-Kontext hat sich die ursprüngliche Reichweitenmessung daher unter Verwendung zahlreicher, häufig individualisierter Informationen zu einer Reichweitenanalyse mit nicht fest definiertem Umfang entwickelt, die um beliebige Kriterien ergänzt werden kann. Eine Festlegung, ob eine „Reichweitenmessung“ ohne Einwilligung rechtmäßig ist, kann allenfalls für eine genau definierte Konfiguration und Zweckbestimmung getroffen werden. Diese wäre nicht mehr gültig, wenn weitere Informationen über Nutzende oder ein weiteres Auswertungsergebnis hinzukommt.

(90) Selbst wenn es ein einheitliches Verständnis über den Begriff der Reichweitenmessung oder der Reichweitenanalyse gäbe, bestünde zweitens das Problem, dass damit ganz unterschiedliche Zwecke verfolgt werden können. Grundsätzlich wird das Ziel verfolgt, mit Erkenntnissen aus der Vergangenheit Entscheidungen für die Zukunft zu treffen, die sowohl den Interessen der Anbieter:innen des digitalen Dienstes, der Nutzenden oder auch von Dritten dienen können. Reichweitenanalysen von Webseiten werden z. B. eingesetzt, um Geschäftsmodelle zu entwickeln, den Verkaufswert von Werbeflächen zu

[49] Bspw. über eine Suchmaschine, ein soziales Netzwerk, eine andere Webseite oder von der internen Suche.

bestimmen, häufig aufgerufene Inhalte besser zu platzieren, Fehlfunktionen zu erkennen, den Umfang von gesetzlich geregelten Leistungsschutzrechten der Autor:innen veröffentlichter Beiträge zu erfassen und vieles mehr. Der Zweck, für den die „Reichweitenmessung“ verwendet wird, ist allerdings maßgeblich für die Beantwortung der Frage, ob ein ausdrücklich von dem/der Nutzer:in gewünschter digitaler Dienst anzunehmen ist. Selbst die einfache Messung von Besucherzahlen ist daher nicht per se als Bestandteil des Basisdienstes einzustufen, sondern abhängig vom jeweils konkret verfolgten Zweck. Die fehlerfreie Auslieferung der Webseite kann beispielsweise vom Nutzerwunsch umfasst sein, während die Wirtschaftlichkeit von Werbeanzeigen im Regelfall nur den primären Interessen des Webseitenbetreibers dient.

(91) Zusatzprobleme ergeben sich dadurch, dass von den Anbieter:innen der digitalen Dienste mit dem Einsatz einzelner Cookies häufig mehrere Zwecke verfolgt werden und eingebundene Drittdienstleister wiederum weitere eigene Zwecke mit den Informationen aus den Cookies verfolgen können.

(92) Bei der Einbindung von Drittdiensten besteht drittens das Problem, dass der Vorgang des Speicherns von Informationen auf dem Endgerät der Nutzenden und das Auslesen dieser Informationen häufig nicht nur einem Dienst mit einer klar bestimmbaren Funktion zuzuordnen ist, sondern die Basis für mehrere Dienste darstellt. Als Beispiel bieten sich hier die Anbieter von Consent-Management-Plattformen an. Deren Produktpalette umfasst in vielen Fällen beispielsweise auch Marketingdienste. Beim Einsatz eines CMP wird häufig ein Cookie gesetzt, der eine eindeutige Benutzerkennung aufweist, obwohl dies für den Zweck der Speicherung des Einwilligungsstatus nicht erforderlich ist. In diesem Fall drängt sich die Vermutung auf, dass derselbe Cookie auch für den Marketingdienst verwendet werden kann. Ob dies dann der Fall ist, kann von Nutzer:innen der Webseite nicht unmittelbar festgestellt werden.

(93) Im Folgenden werden aus Sicht der Aufsichtsbehörden die maßgeblichen Prüfkriterien zusammengefasst, die von Anbieter:innen von digitalen Diensten bei der Bewertung berücksichtigt werden sollten, ob eine Ausnahme gemäß § 25 Abs. 2 Nr. 2 TDDDG vorliegt.

(94) Maßgebliche Kriterien für die Bestimmung des von Endnutzer:innen ausdrücklich gewünschten digitalen Dienstes:

- Granulare Festlegung, für welche Funktion des Telemediendienstes welcher konkrete Speicher- und Auslesevorgang von Informationen auf dem Endgerät erfolgt.
- Bestimmung, wessen primären Interessen diese Funktion dient: den eigenen Interessen der Anbieter:innen, den Interessen der Nutzenden der Webseite, den Interessen des eingebundenen Drittdienstleisters oder den Interessen von Dritten.

(95) Maßgebliche Kriterien für die Bestimmung der unbedingten Erforderlichkeit:

- Zeitpunkt der Speicherung – Wann darf der Auslese- und Speichervorgang stattfinden?

  Der Speicher- und Auslesevorgang von Informationen auf dem Endgerät darf erst dann beginnen, wenn die konkrete Funktion des digitalen Dienstes von Nutzenden tatsächlich in Anspruch genommen wird.

- Inhalt der Informationen – Welche Informationen werden gespeichert und ausgelesen?

  Die gespeicherten und ausgelesenen Informationen müssen bezogen auf die granular festgelegte Funktion des digitalen Dienstes unbedingt erforderlich sein. Insbesondere beim Einsatz

von Cookies ist nicht allgemein darauf abzustellen, dass ein Cookie gesetzt oder ausgelesen wird, sondern die im Cookie gespeicherte Informationen ist maßgeblich.

- Dauer der Speicherung der Informationen – Wie lange werden Informationen auf den Endgeräten gespeichert und für welchen Zeitraum können sie ausgelesen werden?

  Der Zeitraum der Speicherung darf nur so lang gewählt werden wie für die Umsetzung der granularen Funktion des digitalen Dienstes erforderlich. In Bezug auf den Einsatz von Cookies ist dieser Zeitraum durch deren Laufzeit von vornherein festzulegen. Grundsätzlich sind Session-Cookies eher erforderlich als langlebige Cookies.

- Auslesbarkeit der Informationen – Für wen sind Informationen vom Endgerät auslesbar und verwertbar?

  Werden Informationen auf dem Endgerät der Nutzenden bei der Inanspruchnahme eines digitalen Dienstes gespeichert, muss technisch sichergestellt werden, dass diese nachfolgend grundsätzlich nur von den Betreiber:innen der jeweiligen Webseite ausgelesen werden können. Bei Third-Party-Cookies ist dies gerade nicht der Fall, so dass sichergestellt sein muss, dass Drittdienstleister die ausgelesenen Informationen grundsätzlich ausschließlich für die von Nutzenden aufgerufenen Webseite verwenden.

IV. Rechtmäßigkeit der Verarbeitung gemäß DS-GVO

(96) Wenn durch Anbieter:innen von digitalen Diensten personenbezogene Daten (die z. B. unter Verwendung von Cookies und ähnlichen Technologien erhoben wurden) verarbeitet werden, beispielsweise um das individuelle Verhalten von Nutzenden zu verfolgen, sind hierfür die allgemeinen Vorgaben der DS-GVO zu beachten. Zur Vereinfachung wird für Verarbeitungsprozesse zur Verfolgung des Verhaltens von Nutzenden nachfolgend der Begriff „Tracking“ verwendet.[50]

(97) Grundsätzlich sind verschiedenen Vorgänge zu unterscheiden. Im Kontext von Onlineangeboten ist dabei zunächst die Speicherung von Informationen in der Endeinrichtung oder der Zugriff auf Informationen die bereits in der Endeinrichtung gespeichert sind und der sich anschließenden Verarbeitung personenbezogener Daten zu unterscheiden. Die Speicherung von Informationen in der Endeinrichtung oder der Zugriff auf Informationen die bereits in der Endeinrichtung gespeichert sind, unterfällt dem Anwendungsbereich des TDDDG. Unberührt davon bleibt die Frage der Rechtmäßigkeit der nachfolgenden Verarbeitung von personenbezogenen Daten, die als Folge des Auslesens von Informationen aus den Endgeräten erlangt und anschließend verarbeitet werden. Diese unterliegt den Anforderungen des Datenschutzrechts, das heißt insbesondere der DS-GVO.[51]

(98) Erfordert die Speicherung von oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, die Einwilligung der Nutzenden nach § 25 Abs. 1 TDDDG, müssen sämtliche Wirksamkeitsvoraussetzungen gemäß der Verordnung (EU) 2016/679 vorliegen. Sofern keine Einwilligung erteilt wurde oder Wirksamkeitsmängel der Einwilligung nach § 25 Abs. 1 TDDDG festgestellt werden,

[50] Dieses Begriffsverständnis wird auch von den europäischen Aufsichtsbehörden zugrunde gelegt, s. EDSA, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, Rn. 4.
[51] Drucksache 19/27441, S. 38.

wirkt dies auf die nachgelagerte Verarbeitung fort. Datenverarbeitungen, die nachgelagert auf der Speicherung von oder durch den Zugriff auf Informationen in der Endeinrichtung basieren, können nur rechtmäßig erfolgen, wenn die vorgelagerte Verarbeitung nach dem TDDDG rechtmäßig ist.[52] In derartigen Konstellationen muss im Rahmen der Rechtmäßigkeit der Datenverarbeitung nach der DS-GVO inzident geprüft werden, ob die vorgelagerten Vorgänge der Speicherung oder des Auslesens von Informationen rechtmäßig stattgefunden hat. Denn schon das Einfallstor, um die nachgelagerte Verarbeitung überhaupt durchführen zu können, wurde von den Nutzenden nicht „geöffnet". Dies muss ferner gelten, wenn eine Einwilligung zwar erteilt wurde, diese jedoch unter Wirksamkeitsmängeln leidet. Auch hier liegt keine Konstellation vor, die eine nachgelagerte Verarbeitung nach der DS-GVO legitimieren könnte.

(99) DS-GVO und TDDDG haben zwar unterschiedliche Schutzgegenstände und -zwecke, gleichzeitig aber überschneidende Anwendungsbereiche.[53] Die Unterschiede in der Schutzrichtung müssen bei der rechtlichen Betrachtung der verschiedenen Zugriffs- und Verarbeitungsphasen berücksichtigt, können aber, wie oben aufgezeigt, nicht komplett isoliert voreinander betrachtet werden.

(100) Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn mindestens eine der Bedingungen des Art. 6 Abs. 1 DS-GVO erfüllt ist. Sämtliche der in dieser Norm genannten Rechtsgrundlagen stehen gleichrangig und gleichwertig nebeneinander. Für die Verarbeitung personenbezogener Daten durch nicht-öffentliche Verantwortliche bei der Erbringung von digitalen Diensten kommt es grundsätzlich in Betracht, sich auf eine Einwilligung gemäß Art. 6 Abs. 1 lit. a) DS-GVO, auf vertragliche Verpflichtungen nach Art. 6 Abs. 1 lit. b) DS-GVO oder auf überwiegende berechtigte Interessen gemäß Art. 6 Abs. 1 lit. f) DS-GVO zu berufen.

(101) Zu beachten ist, dass mit der Einbindung von Drittinhalten auf Webseiten regelmäßig eine Offenlegung personenbezogener Daten an Betreiber:innen des jeweiligen Drittservers verbunden ist. Für diese Datenverarbeitung ist gemäß Art. 6 Abs. 1 DS-GVO eine Rechtsgrundlage erforderlich. Typische Beispiele für solche Drittinhalte sind Werbeanzeigen, Schriftarten, Skripte, Stadtpläne, Videos, Fotos oder Inhalte von Social-Media-Diensten.

Hinweis: Rechenschaftspflicht

Verantwortliche müssen im Rahmen ihrer Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO nachweisen können, dass die Verarbeitung personenbezogener Daten rechtmäßig erfolgt. Dies bedeutet, dass Verantwortliche vorab prüfen und dokumentieren müssen, auf welchen Erlaubnistatbestand sie die Verarbeitung stützen. Die betroffenen Personen müssen gemäß Art. 13 f. DS-GVO über die Rechtsgrundlagen für sämtliche Verarbeitungen ihrer personenbezogenen Daten informiert werden.

1. Art. 6 Abs. 1 lit. a) DS-GVO – Einwilligung

(102) Die formalen und inhaltlichen Anforderungen an eine wirksame Einwilligung ergeben sich sowohl im Anwendungsbereich des § 25 TDDDG als auch im Anwendungsbereich der DS-GVO aus Art. 4 Abs. 1

[52] Leitlinien 01/2020 zur Verarbeitung personenbezogener Daten im Zusammenhang mit vernetzten Fahrzeugen und mobilitätsbezogenen Anwendungen, Version 2.0, Rz. 49 f.
[53] Grages, CR 2021, 834.

Nr. 11 i. V. m. Art. 7 und 8 DS-GVO.[54] Demnach ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

(103) Für die Beurteilung der Wirksamkeit einer Einwilligung sind daher grundsätzlich diejenigen Maßstäbe anzulegen, die bereits oben unter III.2. dargestellt wurden – mit der Maßgabe, dass die Einwilligung durch die betroffene Person zu erteilen ist und die zur Verfügung gestellten Informationen sich eindeutig auf Datenverarbeitungsprozesse (und nicht lediglich den technischen Einsatz von Cookies o. Ä.) beziehen müssen.[55]

2. Art. 6 Abs. 1 lit. b) DS-GVO – Vertrag

(104) Die Verarbeitung personenbezogener Daten des Vertragspartners auf vertraglicher Grundlage gemäß Art. 6 Abs. 1 lit. b) DS-GVO ist nur möglich, wenn die Datenverarbeitung zur Erfüllung eines Vertrages oder im Rahmen vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Mit der Verarbeitung personenbezogener Daten gemäß Art. 6 Abs. 1 lit. b) DS-GVO im Zusammenhang mit der Bereitstellung von Online-Diensten hat sich bereits der Europäische Datenschutzausschuss vertieft beschäftigt. Die Ausführungen in den Leitlinien 2/2019 können daher durch Anbieter:innen von digitalen Diensten als Prüfungsmaßstab herangezogen werden.[56]

3. Art. 6 Abs. 1 lit. c) DS-GVO – Rechtliche Verpflichtung

(105) Die Verarbeitung von personenbezogenen Daten ist gemäß Art. 6 Abs. 1 lit. c) DS-GVO rechtmäßig, wenn sie zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt. Das bedeutet, dass Art. 6 Abs. 1 lit. c) DS-GVO allein keine Verarbeitung personenbezogener Daten rechtfertigen kann, sondern diese muss ergänzend durch eine gesetzliche Rechtsgrundlage – die rechtliche Verpflichtung – erlaubt werden. Erforderlich ist, dass sich die in einer Vorschrift normierte Verpflichtung unmittelbar auf die Datenverarbeitung bezieht. Allein der Umstand, dass ein Verantwortlicher, um irgendeine rechtliche Verpflichtung erfüllen zu können, auch personenbezogene Daten verarbeiten muss, reicht demgegenüber nicht aus.

4. Art. 6 Abs. 1 lit. e) DS-GVO – Wahrnehmung öffentlicher Interessen

(106) Art. 4 Abs. 1 lit. e) DS-GVO rechtfertigt eine Datenverarbeitung personenbezogener Daten, die für die Wahrnehmung einer Aufgabe erforderlich ist und die im öffentlichen Interesse liegt. Ob eine Aufgabe im öffentlichen Interesse besteht, die eine Verarbeitung personenbezogener Daten erfordert, be-

[54] Zur Abgrenzung der Prozesse, siehe bereits oben unter I. und II.2.
[55] Zur Bündelung von Einwilligungen gemäß § 25 Abs. 1 TDDDG und Art. 6 Abs. 1 lit. a) DS-GVO siehe III.1.e).
[56] EDSA, Leitlinien 02/2019 zur Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO im Zusammenhang mit der Bereitstellung von Online-Diensten für betroffene Personen, Version 2.0, Rn. 48 ff.

stimmt jedoch nicht der Verantwortliche selbst. Sowohl lit. e) als auch lit. c) können als „direkte“ Rechtsgrundlage nicht herhalten, vielmehr ist der eigentliche Erlaubnistatbestand in der „Rechtsgrundlage für die Verarbeitungen“ der Union oder des Mitgliedstaats zu sehen. Die Datenverarbeitung muss durch die gesetzliche Rechtsgrundlage erlaubt werden, die sie nur zulässt, wenn sie für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt. Dieser Zweck der Datenverarbeitung muss wiederum nach Abs. 3 S. 2 in der Rechtsgrundlage explizit festgelegt sein.[57]

5. Art. 6 Abs. 1 lit. f) DS-GVO – Überwiegende berechtigte Interessen

(107) Bei der Verarbeitung personenbezogener Daten auf der Grundlage des Art. 6 Abs. 1 lit. f) DS-GVO ist zu berücksichtigen, dass die Vorschrift keinen Auffangtatbestand darstellt. Sie kann daher gleichwertig neben den anderen Erlaubnistatbeständen herangezogen werden.

(108) Die Verarbeitung ist nach Art. 6 Abs. 1 lit. f) DS-GVO rechtmäßig, wenn dies zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Ob die Voraussetzungen des Art. 6 Abs. 1 lit. f) DS-GVO erfüllt sind, ist anhand einer dreistufigen Prüfung zu ermitteln:

1. Stufe: Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten
2. Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung dieses Interesses
3. Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall

(109) Im Kontext des Trackings sind in der Praxis nur in wenigen Konstellationen die Voraussetzungen des Art. 6 Abs. 1 lit. f) DS-GVO erfüllt.

(110) Die Interessenabwägung im Rahmen des Art. 6 Abs. 1 lit. f) DS-GVO verlangt eine substantielle Auseinandersetzung mit den Interessen, Grundrechten und Grundfreiheiten der Beteiligten und muss auf den konkreten Einzelfall bezogen sein. Obwohl pauschale Feststellungen, dass eine Datenverarbeitung gemäß Art. 6 Abs. 1 lit. f) DS-GVO zulässig sei, diese gesetzlichen Anforderungen nicht erfüllen, sind diese häufig in Datenschutzerklärungen von Diensteanbieter:innen zu finden.

(111) Darüber hinaus ist in Fällen, in denen Drittdienstleister beim Tracking als Auftragsverarbeiter eingebunden werden, darauf zu achten, ob diese Dienstleister Daten der betroffenen Personen auch zu eigenen Zwecken verarbeiten (z. B. um eigene Dienste zu verbessern oder Interessensprofile zu erstellen). In diesem Fall – und selbst wenn sich der Drittdienstleister sich dies nur abstrakt vorbehält – wird der Rahmen einer Auftragsverarbeitung nach Art. 28 DS-GVO überschritten. Für die Übermittlung personenbezogener Daten – und sei es nur der IP-Adresse – an diese Drittdienstleister kann Art. 6 Abs. 1 lit. f) DS-GVO sodann in der Regel keine wirksame Rechtsgrundlage bilden.

(112) Da diese Rechtsgrundlage regelmäßig nur im Einzelfall und nur bei einer entsprechend aussagekräftigen Abwägung herangezogen werden kann, wird die Prüfung der Voraussetzungen in dieser Orientierungshilfe nicht weiter vertieft.

[57] Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht 1. Auflage 2019, Rn. 70, 71.

6. Übermittlungen personenbezogener Daten an Drittländer

(113) Zu beachten ist schließlich, dass sich die vorgenannte Rechtmäßigkeitsprüfung lediglich auf die Verarbeitung der Daten innerhalb des Europäischen Wirtschaftsraums bezieht. Stets muss daher zusätzlich geprüft werden, ob es bei der jeweiligen Datenverarbeitung zu einer Übermittlung personenbezogener Daten in Drittländer kommt. Dies ist insbesondere bei der Einbindung von Dritt-Inhalten, die durch große Anbieter bereitgestellt werden, oft der Fall. Problematisch ist dies insbesondere, wenn für diese Länder kein Angemessenheitsbeschluss der europäischen Kommission besteht.[58] Der Europäische Gerichtshof hat mit seinem Urteil vom 16. Juli 2020 in der Rechtssache „Schrems II“ (C-311/18) die hohen Hürden für den datenschutzkonformen Transfer personenbezogener Daten in Drittländer verdeutlicht.

(114) Eine Übermittlung von personenbezogenen Daten in Drittländer ohne wirksamen Angemessenheitsbeschluss der EU-Kommission hinsichtlich des Datenschutzniveaus gemäß Art. 45 DS-GVO darf daher nur vorbehaltlich geeigneter Garantien, wie z. B. Standarddatenschutzklauseln, oder bei Vorliegen eines Ausnahmetatbestandes für bestimmte Fälle gemäß Art. 49 DS-GVO erfolgen. Zu beachten ist, dass der reine Abschluss von Standarddatenschutzklauseln wie den von der EU-Kommission beschlossenen Standardvertragsklauseln nicht ausreicht. Es ist darüber hinaus im Einzelfall zu prüfen, ob das Recht oder die Praxis des Drittlandes den durch die Standardvertragsklauseln garantieren Schutz beeinträchtigen und ob ggf. ergänzende Maßnahmen zur Einhaltung dieses Schutzniveaus zu treffen sind. Eine detaillierte Anleitung zum Vorgehen bei der erforderlichen Prüfung hat der Europäische Datenschutzausschuss veröffentlicht.[59] Gerade im Zusammenhang mit der Einbindung von Dritt-Inhalten und der Nutzung von Tracking-Dienstleistungen werden allerdings oft keine ausreichenden ergänzenden Maßnahmen möglich sein. In diesem Fall dürfen die betroffenen Dienste nicht genutzt, also auch nicht in die Webseite eingebunden werden.[60] Personenbezogene Daten, die im Zusammenhang mit der regelmäßigen Nachverfolgung von Nutzerverhalten auf Webseiten oder in Apps verarbeitet werden, können grundsätzlich nicht auf Grundlage einer Einwilligung nach Art. 49 Abs. 1 lit. a) DS-GVO in ein Drittland übermittelt werden. Umfang und Regelmäßigkeit solcher Transfers widersprechen regelmäßig dem Charakter des Art. 49 DS-GVO als Ausnahmevorschrift und den Anforderungen aus Art. 44 S. 2 DS-GVO.[61]

V. Gestaltung von Einwilligungsbannern

(115) Die Abfrage einer Einwilligung erfolgt in der Praxis regelmäßig dadurch, dass beim ersten Aufruf einer Webseite oder einer App ein Banner oder ähnliches grafisches Element mit Informationen und Schaltflächen angezeigt wird. Mit solchen Einwilligungsbannern wird seit der Umsetzung der ePrivacy-Richt-

[58] Zur Situation in den USA s. DSK Anwendungshinweise zum Angemessenheitsbeschluss der EuropäischenKommission zum Datenschutzrahmen EU-USA (EU-US Data Privacy Framework) vom 10. Juli 2023. Damit liegt jetzt ein Angemessenheitsbeschluss vor.

[59] EDSA, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.

[60] Vgl. die Anwendungsfälle 6 und 7 des Anhangs 2 der Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0.

[61] EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49 der Verordnung 2016/679, S. 4.

linie im Telekommunikation-Telemedien-Datenschutzgesetz (jetzt: TDDDG) meist sowohl eine Einwilligung für den Einsatz von Cookies und ähnlichen Technologien gemäß § 25 Abs. 1 TDDDG als auch für nachfolgende Datenverarbeitungsprozesse gemäß Art. 6 Abs. 1 lit. a) DS-GVO abgefragt.

(116) Nicht jeder Einsatz von Cookies oder das anschließende Tracking ist per se einwilligungsbedürftig. Daher sollten entsprechende Einwilligungsbanner nur eingesetzt werden, wenn tatsächlich eine Einwilligung notwendig ist. Andernfalls entsteht der missverständliche Eindruck, dass die betroffenen Personen eine Wahl haben und mit ihrer Entscheidung die technischen Prozesse und Datenverarbeitungen beeinflussen können, obwohl dies nicht gegeben ist.

1. Allgemeine Anforderungen

(117) Damit eine wirksame Einwilligung über ein Einwilligungsbanner entsprechend der oben genannten Kriterien für § 25 Abs. 1 TDDDG und für Art. 6 Abs. 1 lit. a) DS-GVO eingeholt werden kann, sind insbesondere folgende Hinweise zu beachten:

(118) Beim erstmaligen Öffnen einer Webseite oder App erscheint in der Regel, unabhängig davon, ob die Startseite oder eine Unterseite aufgerufen wird, das Einwilligungsbanner beispielsweise als eigenes HTML-Element. In der Regel besteht dieses Element aus einer Übersicht aller einwilligungsbedürftigen Zugriffe auf die Endeinrichtung entsprechend § 25 Abs. 1 TDDDG und aller Verarbeitungsvorgänge, die auf die Rechtsgrundlage Art. 6 Abs. 1 lit. a) DS-GVO gestützt werden. Hierbei müssen die beteiligten Akteure[62] und deren Funktion ausreichend erklärt werden und über ein Auswahlmenü aktiviert werden können. Aktivieren bedeutet in diesem Zusammenhang, dass die Auswahlmöglichkeiten nicht „aktiv“ voreingestellt sein dürfen.

(119) Die Informationen können entsprechend dem Mehrebenenansatz des EDSA gestuft erteilt werden, auf erster Ebene sind jedoch im Regelfall folgende Informationen erforderlich:

- konkrete Zwecke der Verarbeitung,
- wenn individuelle Profile angelegt und mit Daten von anderen Webseiten zu umfassenden Nutzungsprofilen angereichert werden,
- wenn Daten auch außerhalb des EWR verarbeitet werden und
- an wie viele Verantwortliche die Daten offengelegt werden.

(120) Sofern auf der Webseite Drittdienste eingesetzt werden, ist es nicht ausreichend, wenn allgemein darauf hingewiesen wird, dass Informationen an „Partner“ weitergegeben werden. Sollten die Drittdienste beispielsweise für die Zwecke des Nutzertrackings, Erstellung von Nutzerprofilen insbesondere für Marketingzwecke und individualisierte Werbeeinblendungen auf der Webseite eingesetzt werden, genügt eine Information, dass die Drittdienste „die Informationen möglicherweise mit weiteren Daten zusammenführen“ nicht. Eine informierte Einwilligung erfordert in diesem Fall, die Zwecke der Verarbeitung konkret zu erläutern, insbesondere darauf hinzuweisen, wenn individuelle Profile angelegt und mit Daten von anderen Webseiten zu umfassenden Nutzungsprofilen angereichert werden. Werden Drittdienstleister eingebunden, sind diese einzeln zu benennen. Als Mindestanforderung wird die

[62] siehe Fußnote 30, S. 13.

Zweckbeschreibung erwartet, die von den jeweiligen Drittdienstleistern z. B. in den Nutzungsbedingungen bereitgestellt werden.

(121) Während das Einwilligungsbanner angezeigt wird, werden zunächst keine weitergehenden Skripte einer Webseite oder einer App, die potenziell auf die Endgeräte der Nutzenden zugreifen (TDDDG) oder durch die personenbezogene Daten verarbeitet werden (DS-GVO) und insbesondere auch keine Inhalte von fremden Servern geladen, soweit eine Einwilligung hierfür erforderlich ist. Der Zugriff auf Impressum und Datenschutzerklärung darf durch das Einwilligungsbanner nicht behindert werden.

(122) Erst wenn Nutzer:innen ihre Einwilligung(en) durch eine aktive Handlung, wie zum Beispiel das Setzen von Häkchen im Einwilligungsbanner oder den Klick auf eine Schaltfläche abgegeben haben, dürfen Informationen auf den Endgeräten gespeichert oder aus diesem ausgelesen werden, sowie die einwilligungsbedürftige Datenverarbeitung tatsächlich stattfinden.

(123) Sofern eine Einwilligung entsprechend § 25 Abs. 1 TDDDG und für eine nachfolgende Verarbeitung nach Art. 6 Abs. 1 lit. a) DS-GVO durch eine Handlung erteilt werden soll, ist darüber zu informieren.

(124) Eine Ablehnfunktion auf erster Ebene ist aus Sicht der Aufsichtsbehörden nicht generell erforderlich, sondern nur dann, wenn Nutzer:innen mit dem Einwilligungsbanner interagieren müssen, um den Besuch der Webseite fortzusetzen. Sofern durch das Banner keine Webseitenbereiche versperrt und die Inhalte zugänglich sind, mithin keine Aktion der Nutzer:innen erforderlich ist, kann eine Ablehnmöglichkeit auf erster Ebene entbehrlich sein. Dabei ist zu berücksichtigen, dass sich Einwilligungsbanner je nach genutzten Endgeräten und Browsern unterschiedlich angezeigt werden und sich entsprechend unterschiedlich auswirken können. Sofern nicht beispielsweise eine Nutzung der Webseite mit mobilen Endgeräten technisch ausgeschlossen wird, darf das Einwilligungsbanner auch auf kleinen Displays nicht dazu führen, dass Webseitenbereiche versperrt werden oder Inhalte nicht zugänglich sind.

(125) Weiterhin ist eine Ablehnfunktion auf erster Ebene nicht erforderlich, wenn die Einwilligung erst auf einer anderen Ebene erteilt werden kann. Es ist daher eine Frage der Gestaltung des Einwilligungsbanners und eine Einzelfallbetrachtung. Jedoch sind im Hinblick auf gängige Ausgestaltungen der Einwilligungsbanner sehr häufig die Voraussetzungen erfüllt, die eine Ablehnfunktion auf erster Ebene erfordern.

(126) Da eine Einwilligung widerruflich ist, muss eine entsprechende Möglichkeit zur Ausübung des Widerrufs implementiert werden. Der Widerruf muss so einfach möglich sein wie die Erteilung der Einwilligung, Art. 7 Abs. 3 S. 4 DS-GVO.[63]

2. Konkrete Gestaltung von Einwilligungsbannern

(127) Es gibt keinen allgemeinen Standard für die Gestaltung von Einwilligungsbannern in Bezug auf Farbe, Größe oder Kontraste, sodass ein gewisser Spielraum für Verantwortliche verbleibt. Eine Verhaltenssteuerung durch die Gestaltung, die allgemein als Nudging bezeichnet wird, ist daher nicht generell unzulässig. Sie findet jedoch dort ihre Grenzen, wo die Voraussetzungen an eine wirksame Einwilligung im Sinne von Art. 4 Nr. 11 und Art. 7 DS-GVO nicht mehr erfüllt sind. Sofern diese Grenze überschritten ist, ist von einem unzulässigen Nudging auszugehen.

[63] Siehe hierzu Kapitel III. 2. g) “Möglichkeit zum Widerruf der Einwilligung”.

a) Allgemein

(128) Die Prüferfahrungen der Aufsichtsbehörden zeigen, dass ein unzulässiges Nudging in der Regel nicht durch ein einziges Gestaltungsmerkmal entsteht, sondern mehrere Gestaltungsaspekte zusammenwirken.

(129) In den meisten Fällen wird insbesondere das Kriterium der Freiwilligkeit in diesem Kontext von Bedeutung sein. Es kann aber auch die Frage, ob eine informierte Einwilligung eingeholt wird, durch die Gestaltung tangiert werden, beispielsweise durch irreführende Informationen, bewusst verharmlosende Sprache oder eine Informationsüberlastung.

(130) Zur Erfüllung des Merkmals der Freiwilligkeit ist es erforderlich, dass eine Wahlmöglichkeit deutlich erkennbar und auch tatsächlich möglich ist. Allein eine unterschiedliche Farbwahl muss nicht zwangsläufig dazu führen, dass die Freiwilligkeit abzulehnen ist.

(131) Sofern jedoch die alternative Option zur Einwilligung nicht deutlich als solche erkennbar ist, weil diese beispielsweise im Einwilligungstext eingebettet ist, ohne besonders hervorgehoben zu sein, außerhalb des Einwilligungsbanners platziert ist oder aufgrund von Kontrasteinstellungen und/oder Schriftgröße praktisch unlesbar für Nutzer:innen ist, kann die Möglichkeit der Verweigerung der Einwilligung regelmäßig nicht mehr als gleichwertig angesehen werden. Eine Freiwilligkeit wäre dann nicht mehr gegeben.

(132) Einwilligungsbanner sollten daher von den Verantwortlichen so ausgestaltet werden, dass Nutzer:innen seine/ihre Handlungsoptionen als solche auf einen Blick erkennen können. Dies muss unabhängig von der Bildschirmgröße des genutzten Endgerätes gewährleistet werden.

(133) Für die Bewertung ist generell eine Einzelfallbetrachtung erforderlich, da am konkreten Fall zu beurteilen ist, ob die Voraussetzungen an eine rechtswirksame Einwilligung noch erfüllt sind. Zur weiteren Orientierung können die Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them[64] herangezogen werden, die überwiegend auf den Webseitenkontext übertragen werden können.

b) Ablehnoption

(134) Die Ablehnoption muss als Alternative zur Einwilligung eindeutig erkennbar, leicht wahrnehmbar und unmissverständlich sein

(135) Die Möglichkeit keine Einwilligung zu erteilen, muss eindeutig als gleichwertige Alternative zur Option „Einwilligung erteilen“ dargestellt werden. Dies ist anzunehmen, wenn sich z. B. neben einem Button „Einwilligung erteilen“ ein insbesondere in Größe, Farbe, Kontrast und Schriftbild vergleichbarer Button „Weiter ohne Einwilligung“ finden lässt.

(136) Entscheidend ist, dass die Alternative zur Einwilligung als solche von Nutzer:innen wahrgenommen werden kann. Nicht ausreichend ist es beispielsweise, wenn die Möglichkeit abzulehnen außerhalb des Einwilligungsbanners auf der Webseite dargestellt ist oder dies im Fließtext des Banners ohne deutliche optische Hervorhebung oder sprachliche Kenntlichmachung in den Hintergrund tritt, während die

[64] EDSA, Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-32022-dark-patterns-social-media_en.

Möglichkeit der Einwilligungserteilung prominent als Button außerhalb des Fließtextes erscheint. Auch ein identischer Button, der allerdings erst nach Scrollen durch den Einwilligungstext ersichtlich ist, während die Möglichkeit zur Einwilligung direkt zu Beginn des Banners sichtbar ist, ist nicht als gleichwertige Alternative leicht wahrnehmbar.

(137) Wird neben der Schaltfläche zur Einwilligung eine Schaltfläche zum Ablehnen der Einwilligung angeboten, muss die Bezeichnung unmissverständlich sein, sodass Nutzer:innen wissen, dass sie keine Einwilligung erteilen. Dies kann durch eine kurze und prägnante Beschriftung abgebildet werden. Eine Schaltfläche „Einstellungen oder Ablehnen“, die zu einer weiteren Ebene des Banners führt, ist an dieser Stelle nicht ausreichend.

VI. Betroffenenrechte

(138) Werden beim Betrieb einer Webseite personenbezogene Daten insbesondere durch Cookie-IDs, IP-Adressen, Account-Daten oder Eingaben in Formularen personenbezogene Daten verarbeitet, sind die Betroffenenrechte gemäß Art. 12 ff. DS-GVO einzuhalten. Das TDDDG enthält mit Ausnahme der Informationspflicht gemäß § 19 Abs. 3 TDDDG keine spezifischen Regelungen. Im Folgenden werden nicht alle Betroffenenrechte umfassend dargestellt, sondern ausschließlich aus der Praxis bekannte spezifische Probleme im Zusammenhang mit digitalen Diensten thematisiert.

1. Informationspflichten gemäß Art. 13 f. DS-GVO

(139) Die Formulierung „Information des Endnutzers“ in § 25 Abs. 1 S. 2 TDDDG verweist auf die Informationspflichten gemäß Artikel 13 und 14 der DS-GVO.

(140) Die Grundsätze einer fairen und transparenten Datenverarbeitung machen es erforderlich, dass die betroffene Person über die Existenz des Verarbeitungsvorgangs und seine Zwecke unterrichtet wird (ErwG 60). Zwar ergibt sich aus der ePrivacy-Richtlinie ein direkter Verweis auf die Informationspflichten der Artikel 13 und 14 DS-GVO nicht, gleichwohl findet sich in der Richtlinie die Formulierung „umfassende Informationen“, die gemäß der Richtlinie 95/46/EG und damit der DS-GVO erteilt werden müssen. Der Wortlaut des § 25 Abs. 1 S. 2 TDDDG spricht zudem von „Information“ und „Einwilligung“, also von zwei separaten Aspekten der DS-GVO. Sollte der Begriff der Information sich lediglich auf eine informierte Einwilligung beziehen, wäre es ausreichend gewesen zu fordern, dass die Einwilligung gemäß der Verordnung (EU) 2016/679 erfolgen soll. Dies stellt mit Blick auf den oben genannten Grundsatz der fairen und transparenten Datenverarbeitung die einzige Möglichkeit dar, dieser elementaren Forderung nachzukommen. Daher bedeutet dies für Prozesse, die auf Grundlage von § 25 Abs. 1 S. 2 TDDDG erfolgen, dass die Informationspflichten der Artikel 13 und 14 DS-GVO einzuhalten sind.

2. Auskunftsrecht gemäß Art. 15 DS-GVO

(141) Im Online-Kontext sind bei der Auskunft an Betroffene die Anforderungen gemäß Art. 15 i.V.m. Art. 12 DS-GVO zu berücksichtigen. Bei der Geltendmachung von Auskunftsansprüchen durch Betroffene ist ein Sonderproblem bekannt. Sofern sich das Auskunftsersuchen auf Webseiten bezieht, die nicht zugangsbeschränkt sind, sodass die Nutzung also keinen Account erfordert, kann der Betreiber der Webseite häufig dem Namen des Auskunftsersuchenden keine Daten zuordnen. In der Regel wird allerdings

ein Auskunftsersuchen unter Nennung des Namens gestellt. In diesen Fällen können vom Verantwortlichen andere eindeutige Identifikationsmerkmale des Nutzers nachgefragt werden, um über diese die Zuordnung eines Datenbestands zu der anfragenden Person zu ermöglichen.[65] Die Abfrage der Daten zur Identifizierung kann der Verantwortliche auf Art. 11 Abs. 2 S. 2 DS-GVO stützen. Eine Abfrage weiterer Informationen setzt allerdings konkrete, einzelfallbezogene und begründete Zweifel an der Identität der Betroffenen voraus.[66] Die Vorschrift berechtigt auch nicht zu einer routinemäßigen Identitätsprüfung.[67]

3. Recht auf Löschung gemäß Art. 17 Abs. 1 DS-GVO

(142) Beinhalten Cookies oder andere auf den Endeinrichtungen der Endnutzenden abgelegte Informationen eine ID, handelt es sich hierbei um personenbezogene Daten. Im datenschutzrechtlichen Sinne verarbeitet werden diese personenbezogenen Daten bei den nachgelagerten Verarbeitungsvorgängen auf den Servern des Betreibers der Webseite oder der eingebundenen Drittdienste. Diesbezüglich gelten die Betroffenenrechte der DS-GVO einschließlich dem Recht auf Löschung gemäß Art. 17 DS-GVO. Derjenige, der das Setzen des Cookies bewirkt hat, ist technisch aber nur bedingt dazu in der Lage, das Cookie mit der ID auf den Endgeräten der Nutzer:innen wieder zu löschen. Eine unabdingbare Voraussetzung ist zunächst, dass die Nutzer:innen die Webseite erneut besuchen, damit der Betreiber theoretisch erneut auf das Endgerät des Nutzers zugreifen kann. Grundsätzlich liegen Informationen die auf den Endgeräten der Nutzer abgelegt worden sind außerhalb des Einflussbereichs des Betreibers der Webseite oder des über den Cookie eingebundenen Anbieters des Drittdienstes. Da es für die Besucher:innen der Webseite technisch sehr einfach ist, Cookies von ihren Endgeräten wieder zu löschen, besteht datenschutzrechtlich diesbezüglich kein Bedarf an einer Löschpflicht des Webseitenbetreibers.

(143) Dessen ungeachtet muss derjenige, der für den Einsatz des Cookies mit der ID verantwortlich ist, diesen mit einer Laufzeit versehen, sodass eine von ihm steuerbare automatische Löschung umgesetzt wird. Die Laufzeit hat sich an dem Grundsatz der Speicherbegrenzung gemäß Art. 5 Abs. 1 lit. e) DS-GVO zu orientieren. In dieser OH Digitale Dienste wird die Speicherdauer von Cookies – unabhängig von einer personenbezogenen ID – in Kap. III.3.c) „Anwendungsbeispiele und Prüfkriterien“ als maßgebliches Kriterium für die Bestimmung der unbedingten Erforderlichkeit gemäß § 25 Abs. 2 Nr. 2 TDDDG relevant. Aus dieser Vorschrift ergibt sich somit regelmäßig, dass alle Cookies mit einer begrenzten Speicherdauer zu versehen sind, sodass sie automatisch gelöscht werden.

---

[65] So auch EDSA, Guidelines 01/2022on data subject rights - Right of access, Rn. 67.
[66] *Bäcker*, in: Kühling/Buchner, DS-GVO/BDSG, 2024, Art. 12 Rn. 30.
[67] *Paal/Hennemann*, in: Paal/Pauly, DS-GVO/BDSG, 2021, Art. 12 Rn. 72.