



Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (Hg.)

Webseiten rechtskonform gestalten

Die Bedeutung von TTDSG, ePrivacy und Datenschutz in der Praxis



Impressum

Herausgeber

AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
www.awv-net.de | info@awv-net.de

Die Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. versteht sich als Netzwerk für Digitalisierung und Bürokratieentlastung. Sie ist ein bundesweites Forum, in dem Antworten auf aktuelle Fragen rund um die wirtschaftliche Gestaltung administrativer Prozesse entwickelt werden.

Verfasser

AWV-Arbeitskreis 4.3 „Weiterentwicklung des Datenschutzrechts“, mit folgenden Autorinnen und Autoren:

Rudi Kramer, Nürnberg (Leiter des AWV-Arbeitskreises 4.3)
Silvia Küpper, Wiesbaden
Yvette Reif, Bonn
Henry Simwinga, Bonn
Marek van Hattem, Neuss

Der Herausgeber geht davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Spezielle Umstände einzelner Fallkonstellationen wurden nicht berücksichtigt. Bitte konsultieren Sie im Zweifelsfall, einen Rechtsanwalt oder einen Datenschutzexperten, um weitere Entscheidungen für Ihre Situation abzuleiten. Bitte beachten Sie auch mögliche Änderungen der Rechtslage bei oder nach Erscheinen dieser Publikation. Der Herausgeber übernimmt weder ausdrücklich oder implizit Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen.

Genderhinweis: Aus Gründen der leichteren Lesbarkeit wird in dieser Publikation nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung in der Regel für alle Geschlechter.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Redaktion: Sara Pour Abbasi, AWV e.V. | Nicole Wingender, AWV e.V.
Layout und Satz: Cora Strasdat, AWV e.V.
Bildquellennachweis Cover: Adobe Stock/pla2na
Eschborn, Februar 2024
AWV-Best.-Nr.: 43241-w

Hinweis

Diese Handreichung ist ein Leitfaden für Websitebetreiber von Klein- und Mittelunternehmen mit einem gewissen Vorwissen im Themenbereich Datenschutzrecht. Grundlegende Informationen zum Thema Datenschutz erhalten Sie beispielsweise über die im Jahr 2022 veröffentlichte Broschüre **„Die DSGVO – Informationen für kleine und mittlere Unternehmen“** des AWW-Arbeitskreises „Datenschutz und Informationssicherheit“.

Zudem möchten Sie darauf hinweisen, dass der Gesetzgeber plant das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) durch ein Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) zu ersetzen. Das Bundesministerium für Digitales und Verkehr hat einen ersten Referentenentwurf dazu bereits veröffentlicht, der eine Reihe von Änderungen aufzeigt, die bisher allerdings nur redaktioneller Art ausformuliert sind. So wird etwa in Artikel 8 dieses Entwurfs unter anderem vorgeschlagen, dass der Begriff „Telemedien“ künftig durch den Begriff „digitale Dienste“ ersetzt werden soll. In diesem Referentenentwurf wird der Änderungsvorschlag wie folgt begründet: „Das europäische Recht, insbesondere der DSA [The Digital Services Act, Anm. d. Red.], deren Durchführung der Hauptzweck des DDG [digitale Dienste Gesetz, Anm. d. Red.] ist, kennt den Telemedienbegriff nicht. Vor dem Hintergrund harmonisierter Vorschriften für einen Binnenmarktes für digitale Dienste bleibt kein Raum für diesen rein national vorgeprägten Begriff.“*

Der Begriff „digitaler Dienst“ entspricht der Definition des Begriffs „Dienst“ nach Art. 1 Abs. 1 b) RL 2015/1535, der eine Dienstleistung der Informationsgesellschaft ist, das heißt, jede allgemein gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung ist darunter zu verstehen.** Es ist daher derzeit noch nicht absehbar, inwieweit sich damit auch der Anwendungsbereich vom Telemedium zum Digitalen Dienst verändern wird.

Wichtig: Daher weisen wir explizit darauf hin, die weitere Entwicklung zu beobachten. Die AWW wird diese Broschüre entsprechend inhaltlich anpassen, wenn sich außerhalb von redaktionellen Änderungen anderweitige Interpretationen und Anwendungsbereiche ergeben.

AWV-Arbeitskreis 4.3 „Datenschutz und Informationssicherheit“
Eschborn im Februar 2024

Die AWW-Publikation „Die DSGVO – Informationen für kleine und mittlere Unternehmen“ finden Sie als PDF-Ausgabe zum kostenlosen Download auf der AWW-Webseite unter:

www.awv-net.de/dsgvo-kmu



* Bundesministerium für Digitales und Verkehr (Hg.): Referentenentwurf, Bearbeitungsstand 01.08.2023, online: https://bmdv.bund.de/SharedDocs/DE/Anlage/Gesetze/Gesetze-20/gesetz-durchfuehrung-verordnung-binnenmarkt-digitale-dienste.pdf?__blob=publicationFile [09.01.2024], ebd. S. 64.

** Vgl. Johannes Zwerschke: Wichtige Änderungen des TTDSG durch das deutsche DSA-Umsetzungsgesetz in Sicht, 05.09.2023, online: <https://www.piltz.legal/news/wichtige-aenderungen-des-ttdsg-durch-das-deutsche-dsa-umsetzungsgesetz-in-sicht> [09.01.2024].



Inhalt

I. Datenschutzrechtliche Anforderungen bei Onlineauftritten und der Einbindung von Cookies	5
II. Die Anforderungen an Websitebetreiber im Einzelnen	8
1. Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)	8
a) Anwendungsbereich des TTDSG	8
b) Anforderungen an Cookies und Co.	9
c) Cookie-/Consent-Banner.....	12
d) Anwendbarkeit von § 25 TTDSG auf Cookies vergleichbare Verfahren, z. B. sog. Browser- oder Device-Fingerprinting	16
2. Datenschutz-Grundverordnung (DSGVO)	17
a) Anwendungsbereich der DSGVO	17
b) Anforderungen der DSGVO an (Online-)Datenverarbeitungen und Verhältnis von DSGVO und TTDSG.....	19
3. Datenschutzerklärung	20
a) Grundprinzipien bei Erstellung der Datenschutzerklärung.....	21
b) Checkliste Datenschutzerklärung	22
III. Sammlung weiterführender Links	27

I. Datenschutzrechtliche Anforderungen bei Onlineauftritten und der Einbindung von Cookies

Bei der Gestaltung von Webseiten sind Anforderungen aus unterschiedlichen rechtlichen Grundlagen zu beachten. Die vorliegende Handreichung konzentriert sich auf die datenschutzrechtlichen Anforderungen sowie diejenigen an den Schutz von Endgeräten, die sich aus europarechtlichen Grundlagen wie der ePrivacy-Richtlinie ergeben.

Basis dieser Anforderungen sind Vorgaben, die sich aus einer Richtlinie der Europäischen Union aus dem Jahr 2002¹ ergeben und die in 2009² nochmal auf europäischer Ebene konkretisiert wurden. Gegenstand dieser Richtlinien sind die Anforderungen an den Schutz der Privatsphäre bei der elektronischen Kommunikation. Auf europäischer Ebene wird die Privatsphäre bei der elektronischen Kommunikation in Art. 7 der Europäischen Grundrechtcharta³ geschützt.

Richtlinien der Europäischen Union müssen zu ihrer Wirksamkeit in das Recht der Mitgliedstaaten umgesetzt werden. In Deutschland erfolgte dies zunächst im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG). Dabei war zwischen Wissenschaft, Aufsichtsbehörden und Politik von Anfang umstritten, ob diese Umsetzung in Deutschland ausreichend erfolgte. Diese Diskussion versuchte der Gesetzgeber mit der Fassung eines Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) zu beenden, das zum 1. Dezember 2021 in Kraft trat.⁴

Im TTDSG wurden Regelungssachverhalte aus dem TKG und TMG zusammengeführt und teilweise neuformuliert. Die TTDSG-Regelungen finden gemäß § 1 Abs. 3 Satz 1 TTDSG Anwendung auf alle Unternehmen und Personen, die im Geltungsbereich dieses Gesetzes eine Niederlassung haben oder Dienstleistungen erbringen oder daran mitwirken oder Waren auf dem Markt bereitstellen. Im TTDSG werden nicht nur datenschutzrechtliche Vorgaben bezogen auf die Nutzung von Telekommunikations- und



- 1 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).
- 2 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.
- 3 In der Europäischen Grundrechtcharta in Artikel 7 heißt es: „Achtung des Privat- und Familienlebens: Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.“ (Amtsblatt der Europäischen Union, C 303/4, 14.12.2007, 50. Jg., online: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:C:2007:303:FULL&from=D> [30.01.2024]).
- 4 Bundesministerium der Justiz, Bundesamt für Justiz (Hg.): Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien, 23.06.2021, online: <https://www.gesetze-im-internet.de/ttdsg/ttdsg.pdf> [08.01.2024].

Telemedienangeboten geregelt, es werden auch Sachverhalte umfasst, die keinen Personenbezug haben, aber dennoch die Privatsphäre tangieren. Dies ist beispielsweise der Fall, wenn Informationen, wie insbesondere Cookies, in Endgeräten gespeichert oder aus diesen ausgelesen werden.

Mit Telekommunikation beschreibt der Gesetzgeber in § 3 Nr. 59 TKG⁵ den technischen Vorgang des Aussendens, Übermittels und Empfangens von Signalen mittels Telekommunikationsanlagen. Mit Telemedien werden elektronische Informations- und Kommunikationsdienste bezeichnet, bei denen es sich nicht um Rundfunk im Sinne des Medienstaatsvertrages und nicht um bestimmte Telekommunikationsdienstleistungen im Sinne des Telekommunikationsgesetzes handelt⁶. Dies gilt für alle Anbieter einschließlich öffentlicher Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird. Der Begriff Telemedien umfasst insbesondere Webseiten und Apps.

Werden bei der Bereitstellung und Nutzung von Telemedien Informationen verarbeitet, die personenbeziehbar sind, gelten zusätzlich die Anforderungen, die sich aus der Datenschutz-Grundverordnung (DSGVO)⁷ ergeben. Zu dieser hat die AWV bereits eine Broschüre veröffentlicht.⁸

Wird im Rahmen der Erstellung bzw. des Betriebens der Webseite ein Dienstleister eingesetzt, ist insofern zu prüfen, ob die Anforderungen der DSGVO an eine Auftragsverarbeitung erfüllt werden. Eine Auftragsverarbeitung liegt vor, wenn ein Dienstleister beauftragt wird, personenbezogene Daten weisungsgebunden zu verarbeiten. Betreibt ein Dienstleister die Webseite im Auftrag, ist mit diesem eine Vereinbarung zur Umsetzung der Anforderungen an eine Auftragsverarbeitung nach den Vorgaben des Art. 28 DSGVO abzuschließen. Auch hierzu informiert die oben genannte AWV-Broschüre zur DSGVO.⁹ Bzgl. der Webseitenerstellung sollte vertraglich fixiert werden, welche Datenfelder mit Personenbezug erstellt werden und welche Cookies oder vergleichbare technische Maßnahmen für welchen Zweck eingesetzt werden sollen.

⁵ Bundesministerium der Justiz, Bundesamt für Justiz (Hg.): Gesetze im Internet, online: https://www.gesetze-im-internet.de/tkg_2021/BJNR185810021.html [08.01.2024].

⁶ § 1 Abs. 1 Satz 1 Telemediengesetz, online: https://www.gesetze-im-internet.de/tmg/_1.html [08.01.2024].

⁷ European Union (Hg.): EUR-lex. Access to European Union law, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679> [08.01.2024].

⁸ Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (Hg.): Die DSGVO – Hinweise für kleine und mittlere Unternehmen, 2022, online: <https://www.awv-net.de/DSGVO-KMU> [08.01.2024].

⁹ ebd.

Daneben gibt es bei Webseiten weitere Informationspflichten, die sich aus berufsrechtlichen und/oder wettbewerbsrechtlichen Gründen ergeben können. Informationen hierzu finden sich bei den jeweiligen Interessensgruppen der Branchen, den jeweiligen berufsständischen Kammern und Interessensvertretungen oder bei Industrie- und Handelskammern.¹⁰

¹⁰ Vgl. bspw. Industrie- und Handelskammer Wiesbaden (Hg.): Rechtliche Pflichten für Websites – Impressum, Datenschutz etc., online: <https://www.ihk.de/wiesbaden/recht/rechtsberatung/internetrecht-und-werbung/internetauftritt-rechtliche-anforderungen-und-pflichten-1255572> [08.01.2024].

II. Die Anforderungen an Websitebetreiber im Einzelnen

Betreiber von Websites, Apps und Co. haben die Vorgaben des TTDSG, insbes. § 25 TTDSG, sowie die Vorgaben der DSGVO zu beachten. Im Folgenden wird erläutert, auf welche Verhaltensweisen des Websitebetreibers die genannten Regelungen bzw. Regelungswerke konkret Anwendung finden, also ihr sachlicher Anwendungsbereich. Zudem wird der Rechtsrahmen dargestellt, der sich aus § 25 TTDSG bzw. der DSGVO ergibt, also was konkret mit den personenbezogenen Daten der Websitenutzer gemacht werden bzw. unter welchen Voraussetzungen beim Einsatz von Cookies und Co. auf deren Endgeräte zugegriffen werden darf.

1. Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)

a) Anwendungsbereich des TTDSG

Das TTDSG enthält „besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und Telemedien“, vgl. § 1 Nr. 2 TTDSG. Anbieter von Telemedien ist nach § 2 Abs. 2 Nr. 1 TTDSG jede natürliche oder juristische Person, die eigene oder fremde Telemedien erbringt, an der Erbringung mitwirkt oder den Zugang zur Nutzung von eigenen oder fremden Telemedien vermittelt.

Telemedien sind nach § 1 Abs. 1 S. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, telekommunikationsgestützte Dienste oder Rundfunk sind (Telemedien). Beispiele für Telemediendienste sind u. a. Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit (z. B. Angebot von Verkehrs-, Wetter-, oder Börsendaten, elektronische Presse, Fernseh-/Radiotext, Teleshopping), Video on Demand, Internet-suchmaschinen, Werbemails, aber auch bereits „einfache“ Website zur Information über zur Information über ein Unternehmen bzw. eine öffentliche Stelle.



b) Anforderungen an Cookies und Co.

Beim Websitebetrieb kommen vielfach Cookies zum Einsatz, die auf den Endgeräten der Nutzer abgelegt und später wieder ausgelesen werden.

Was sind COOKIES?*

Cookies sind kleine Textdateien, die der Webbrowser auf dem Endgerät speichert. Anhand von Cookies erkennt eine Website, wer sie gerade besucht, und kann dadurch Nutzerpräferenzen, wie z. B. Sprach- oder Login-Informationen speichern, damit der Nutzer die Einstellungen nicht immer wieder neu vornehmen bzw. sich immer wieder neu anmelden muss. Beim Onlineshopping verhindern Cookies, dass sich mit jedem Aufruf einer neuen Unterseite im Rahmen des Webangebots der Warenkorb leert. Beim Online-Marketing ermöglicht der Einsatz von Cookies, die Nutzerinteressen auch sitzungsübergreifend zu ermitteln und so möglichst zielgenaue Onlinewerbung auszuspielen. Dabei handelt es sich um sogenannte **persistente Cookies**, die dauerhaft im System des Nutzers hinterlegt werden. Von diesen zu unterscheiden sind sogenannte Session Cookies. **Session Cookies** werden gelöscht, sobald der User nach der Internetsitzung (englisch: Session) den Browser schließt.

Sofern Cookies von der Website gesetzt werden, auf der sich der Nutzer gerade befindet, spricht man von **First Party Cookies**. **Third Party Cookies** sind demgegenüber Cookies, die nicht vom Betreiber der Website, sondern von einem Dritten platziert werden, dessen Inhalte auf der besuchten Website eingebunden sind. „Third Party Cookies“ liefern ein deutlich klareres Bild der Nutzerpräferenzen, denn mit diesen kann nicht mehr nur nachverfolgt werden, wofür der Nutzer sich innerhalb des eigenen Webauftritts interessiert, sondern über verschiedene Onlineangebote hinweg.

* Die Erläuterungen zu den Cookies basieren auf den Ausführungen bei Rolf Schwartmann/Kristin Benedikt/Yvette Reif, Sonderveröffentlichung RDV, 5/2020, online: https://dataagenda.de/wp-content/uploads/2020/10/RDV_5_-Sonderdruck_SchwartmannBenediktReif.pdf [09.01.2024].

Zum Schutz der Privatsphäre des Nutzers bei der Nutzung von beispielsweise PCs, Laptops, Tablets oder Smartphones knüpft § 25 Abs. 1 TTDSG das Setzen und Auslesen von Cookies bzw. vergleichbare Verfahren, z. B. sog. Browser- oder Device-Fingerprinting im Grundsatz an eine vorherige Einwilligung des Nutzers.



Von diesem grundsätzlichen Einwilligungserfordernis sind nach § 25 Abs. 2 TTDSG lediglich zwei Ausnahmen vorgesehen. Praxisrelevant ist v. a. die zweite in § 25 Abs. 2 TTDSG vorgesehene Ausnahme:¹¹

Der Einsatz von Cookies & Co. erfordert keine Einwilligung des Nutzers, sofern diese Cookies unbedingt zur Erbringung eines vom Nutzer ausdrücklich gewünschten Dienstes erforderlich sind.

Als **einwilligungsfrei möglich** werden etwa nachfolgende Kategorien von Cookies angesehen, sofern die **Cookies** nicht für weitere Zwecke verwendet werden:¹²

▶ **User-Input-Cookies (Session-ID)**

Darunter sind Cookies zu verstehen, die für die Dauer einer Sitzung oder in bestimmten Fällen persistente Cookies, deren Gültigkeitsdauer auf wenige Stunden beschränkt ist. Gemeint sind Cookies, die der einheitlichen Verfolgung von Nutzereingaben bei einer Reihe von Nachrichtenaustauschvorgängen mit einem Dienstleister dienen (z. B. Warenkorb-Cookies).

▶ **Authentifizierungs-Cookies**

Darunter sind Cookies für Dienste zu verstehen, bei denen eine Authentifizierung erforderlich ist. Authentifizierungs-Cookies werden verwendet, um den Nutzer zu identifizieren, nachdem er sich angemeldet hat (z. B. beim Onlinebanking). Sie werden benötigt, damit sich der Nutzer beim Aufruf von einzelnen Unterseiten innerhalb des geschützten Bereichs nicht immer wieder erneut authentifizieren muss. Authentifizierungs-Cookies sind in der Regel Sitzungs-Cookies (Session Cookies). Hat der Nutzer aber auf Abfrage bestätigt, dass er angemeldet bleiben möchte, dürfen die Cookies auch über die Sitzung hinaus als sogenannte persistente Cookies gespeichert werden.

▶ **Nutzerorientierte Sicherheits-Cookies**

Ob auch Cookies, die Sicherheitsinteressen der Anbieter dienen, z. B. der Vermeidung von Klickbetrug, ohne Einwilligung des Nutzers verwendet werden dürfen, ist umstritten.

¹¹ Vgl. ggf. ergänzend auch: § 25 Abs. 2 Nr. 1 TTDSG: „Die Einwilligung nach Absatz 1 ist nicht erforderlich, 1. wenn der alleinige Zweck der Speicherung von Informationen in der Endrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist.“

¹² Art.-29-Datenschutzgruppe, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, WP 194 v. 7.6.2012, S. 7 ff., dort finden sich auch noch weitere Beispiele einwilligungsfrei möglicher Cookies.

► **Cookies zur Anpassung der Benutzeroberfläche**

Solche Cookies werden verwendet, um die nicht mit einer anderen dauerhaften Kennung (z. B. einem Benutzernamen) verknüpfte Einstellungen (z. B. Einstellung zur Sprache) für einen mehrere Webseiten umfassenden Dienst zu speichern.

Soweit auf einer Website nur einwilligungsfrei mögliche Cookies eingesetzt werden, braucht es kein sogenanntes Cookie-Banner oder auch „Consent-banner“, um eine Einwilligung einzuholen. Es genügt, über die eingesetzten Cookies in der Datenschutzerklärung der Website zu informieren.

Regelmäßig als **einwilligungsbedürftig** anzusehen ist insbesondere das Setzen bzw. Auslesen von **Werbe-Cookies** oder sonstige Endgerätzugriffe zum Zwecke der Informationsgewinnung zu Werbezwecken. Die Generierung von Werbeeinnahmen durch Ausspielen interessenbasierter Werbung steht in keinem funktionalen Zusammenhang zur Erbringung des Telemediendienstes. Zwar mag es aus Sicht des Diensteanbieters zur Finanzierung seines Geschäftsmodells ggf. wirtschaftlich erforderlich sein, bestimmte – typischerweise werbliche – Zugriffe und anschließende Datenverarbeitungen durchzuführen. Eine bloß wirtschaftliche Erforderlichkeit ist im Rahmen von § 25 Abs. 2 Nr. 2 TTDSG aber nicht als ausreichend anzusehen.



**Sind ENDGERÄTZUGRIFFE zur Reichweitenmessung/
Webanalyse einwilligungsfrei möglich?**

Viele Websitebetreiber möchten analysieren, welche Inhalte des Internetangebots besonders häufig gelesen werden, welche Fehler auftreten oder an welcher Stelle die Besucher die Seite verlassen usw. (sog. Reichweitenmessung). Inwieweit zu diesen Zwecken durchgeführte Endgerätzugriffe unbedingt erforderlich im Sinne von § 25 Abs. 2 Nr. 2 TTDSG sind, ist nicht abschließend geklärt. Nach Auffassung der französischen Datenschutz Behörde CNIL soll die Regelung eine „einfache“ Webanalyse rechtfertigen können, vorausgesetzt, diese wird in anonymisierter Form vom Websitebetreiber selbst vorgenommen und dient ausschließlich der Fehlerbehebung, der Optimierung der technischen Performance oder auch der Analyse der konsultierten Inhalte.*

Unstreitig kommen Verfahren zur Reichweitenmessung jedenfalls dann einwilligungsfrei in Betracht, sofern ein Endgerätzugriff vermieden und die Analyse z. B. im Wege der **Logfile-Analyse** oder des **Server-Side-Tracking** ohne Cookies durchgeführt wird.**

* Vgl. CNIL (Hg.): Lignes directrices „cookies et autres traceurs“, Rz. 50 f.; ähnlich auch die italienische Datenschutzaufsicht Garante per la protezione dei dati personali, Linee guida cookie e altri strumenti di tracciamento – 10.6.2021.

** Vgl. hierzu Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (Hg.): FAQ. Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0.1 (März 2022), S. 13 ff. Auch die spanische Datenschutzaufsicht aepd sieht für eine moderate Reichweitenmessung ohne vorherige Einwilligung in engen Grenzen eine Möglichkeit „Guía Uso de cookies para herramientas de medición de audiencia“, Januar 2024, online: <https://www.aepd.es/guias/guia-cookies-analiticas-externas.pdf> [06.02.2024].

Schützt das TTDSG nur NATÜRLICHE PERSONEN?

Anders als durch die DSGVO werden durch § 25 TTDSG **auch juristische Personen geschützt**. Sofern mit dem Zugriff auf ein Endeinrichtung keine personenbezogenen Datenverarbeitungen einhergehen, ist allein das TTDSG maßgeblich.

Gehen mit dem Endgerätezugriff auch **personenbezogene Datenverarbeitungen** einher, kommen insoweit **§ 25 TTDSG und die DSGVO nebeneinander** zur Anwendung.

Ausschließlich nach der DSGVO bestimmt sich die Weiterverarbeitung personenbezogener Daten, welche beim Zugriff auf die Endeinrichtung angefallen sind.



c) Cookie-/Consent-Banner

Einwilligungen im Zusammenhang mit Cookies – und ggf. verbundenen Online-Datenverarbeitungen¹³ – werden üblicherweise mittels einer der Website-Nutzung vorgeschalteten Abfrage eingeholt, die beim ersten Aufruf eingeblendet und in der Praxis als Cookie- oder auch Consent-Banner bezeichnet wird. Banner, mit denen eine Einwilligung nach TTDSG und/oder DSGVO eingeholt werden soll, müssen den Anforderungen genügen, welche die DSGVO an das Vorliegen einer wirksamen Einwilligung stellt (Art. 7 DSGVO, Art. 4 Nr. 11 DSGVO). Für die TTDSG-Einwilligung ergibt sich dies über einen Verweis in § 25 Abs. 1 S. 2 TTDSG.

Wann braucht man kein COOKIE-BANNER?

Wichtig: Einer Cookie-Einwilligung und damit eines Banners bedarf es nicht, sofern nur für die Funktion des gewünschten Dienstes essenzielle Cookies eingesetzt werden. Über diese ist lediglich in der Datenschutzerklärung zu informieren.*

* Vgl. dazu in dieser Publikation den Abschnitt „Anforderungen an Cookies und Co.“ ab S. 9.

Welche konkreten Anforderungen an die Cookie-Banner-Gestaltung zu stellen sind, ist bezogen auf diverse Aspekte strittig. Praxisrelevant im Hinblick auf die Einholung einer wirksamen Einwilligung sind insbesondere die im Folgenden aufgezählten fünf Punkte:

¹³ Siehe Kapitel zur DSGVO in dieser Publikation unter II. 2. a) ab S. 17

1. Unmissverständliche Erklärung oder sonstige eindeutige bestätigende Handlung, dazu gehören

- ▶ keine voreingestellten Ankreuzkästchen, aktive Handlung des Nutzers nötig („Planet49“-Entscheidung¹⁴ des EuGH)
- ▶ keine Einwilligung durch Weitersurfen
- ▶ „maßvolles“ Nudging, das heißt, die Beeinflussung der Nutzerentscheidung durch optische Gestaltung der Schaltflächen ist nur zulässig, solange es „maßvoll“ erfolgt
- ▶ regelmäßig „Reject All“-Button auf erster Ebene des Cookie-Banners nötig (nach Datenschutzkonferenz (DSK))

2. Freiwilligkeit

- ▶ Sog. **Kopplungsverbot** (Art. 7 Abs. 4 DSGVO)

3. Informiertheit

- ▶ Für wirksame Einwilligung nötige, **allgemeine Mindestinformationen sind:**¹⁵
 - Identität des Verantwortlichen
 - Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird
 - (Art der) Daten, die erhoben und verwendet werden
 - Hinweis auf Widerrufsrecht
 - ggf. Informationen über die Verwendung der Daten für eine automatisierte Entscheidungsfindung
 - ggf. Angaben zu möglichen Risiken von Datenübermittlungen in ein Land außerhalb der EU/des EWR ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art. 46 DSGVO



¹⁴ EuGH, Urt. v. 1.10.2019 – C-673/17.

¹⁵ EDSA, Leitlinien 05/2020 zur Einwilligung gem. Verordnung 2016/679, Version 1.1, 04.05.2020, Rn. 64.

- ▶ Bei Einwilligungen in **Cookies zu Werbezwecken** gehören zu den **Mindestinformationen** auch:
 - Angaben zur Funktionsdauer der Cookies und
 - ob Dritte Zugriff auf die Cookies erhalten können.¹⁶
- ▶ Beachtung der **weitergehenden Informationspflichten** (nach Art. 13 f. DSGVO)
- ▶ **Prinzip der gestuften Informationsübermittlung („layered privacy notice“)**
 - Für die Nutzerentscheidung **wesentliche Informationen** gehören regelmäßig unmittelbar auf die **erste Bannerebene** (insbes. Verarbeitungszwecke und ob auch Dritte auf das Endgerät zugreifen bzw. anfallende Informationen im Eigeninteresse verarbeiten).
 - Bezüglich **weiterer Informationen** genügt es, dass diese deutlich sichtbar verlinkt sind bzw. sich auf der nächsten Banner-Ebene befinden.

4. Nachweis der Einwilligung

- ▶ Nach DSK genügt es, nachweisen zu können, dass und welche Prozesse implementiert wurden.



¹⁶ GEuGH, Urf. v. 1.10.2019 – C-673/17 („Planet49“-Entscheidung).

5. Widerruf der Einwilligung

- ▶ Ein Widerruf muss **so einfach wie die Erteilung** der Einwilligung möglich sein (Art. 7 Abs. 3 S. 4 DSGVO).
- ▶ Ein Widerruf muss über einen **„stets sichtbaren“ Direktlink bzw. ein Icon** erteilt werden können (nach DSK).

Siehe hierzu nachfolgende Beispiele:



* Abbildung in Anlehnung an CNIL (Hg.): Délibération n° 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux „cookies et autres traceurs“ (Übersetzung ins Deutsche durch AWV e.V.), online: <https://cnil.fr/sites/cnil/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf> [06.02.2024].

Wer haftet beim CONSENT-BANNER für die Richtigkeit?

Websitebetreiber bleiben auch bei Einsatz sogenannter **Consent-Management-Plattformen (CMP)** verantwortlich für die Wirksamkeit der hierüber eingeholten Erklärungen bzw. die Rechtskonformität der Verarbeitungen im Zusammenhang mit der Website. Zusicherungen des CMP-Anbieters, dass der Websitebetreiber mit seinem Produkt auf der rechtssicheren Seite sei, vermögen allenfalls zu Regressmöglichkeiten im Verhältnis zu diesem zu führen, können den Websitebetreiber aber im Verhältnis zur betroffenen Person bzw. zur Aufsichtsbehörde oder Verbraucherschutzverbänden nicht entlasten.

Daher ist dringend anzuraten, vor dem Einsatz eines Cookie-Banners in Zusammenarbeit mit dem CMP-Anbieter die Rechtskonformität zu prüfen und sicherzustellen.

d) Anwendbarkeit von § 25 TTDSG auf Cookies vergleichbare Verfahren, z. B. sog. Browser- oder Device-Fingerprinting

§ 25 TTDSG regelt nicht nur den Einsatz von Cookies, sondern ist technikneutral. Erfasst werden etwa auch Zugriffe auf Endgeräte durch Apps sowie Gegenstände im Internet der Dinge (Internet of Things – IoT), z. B. Küchen- oder Alarmgeräte. Ob auch alternative Onlinetrackingverfahren von der Norm erfasst werden, wie z. B. das Browser-/Device-Fingerprinting, hängt von deren konkreter Funktionsweise ab, das heißt davon, ob hierzu ein „Zugriff“ im Sinne von § 25 TTDSG auf das Endgerät stattfindet.

Was ist unter FINGERPRINTING zu verstehen?

Beim sogenannten Fingerprinting erfassen die Webserver unterschiedliche Merkmale der Browser der Besucher und ermitteln auf dieser Basis jeweils einen individuellen digitalen Fingerabdruck, mittels dessen die Nutzer – bzw. genauer: deren Browser – später wiedererkannt werden können. Zu den verwendeten Merkmalen zählen etwa Bildschirmauflösungen, Betriebssystemversionen, installierte Schriften oder Spracheinstellungen.



Die nationale DSK lehnt eine umfassende Anwendung des § 25 TTDSG auf derartige Verfahren ab. Sie differenziert zwischen dem Zugriff auf Daten, die beim Abruf eines Telemediendienstes aufgrund von Browsereinstellungen automatisch übermittelt und insofern nur noch „passiv“ entgegengenommen werden, und dem Zugriff auf Daten, die vor Entgegennahme „aktiv“, z. B. mittels JavaScript-Code, abgefragt wurden. Nur im letztgenannten Fall liege, so die DSK, ein „Zugriff“ i. S. v. § 25 vor.¹⁷

2. Datenschutz-Grundverordnung (DSGVO)

a) Anwendungsbereich der DSGVO

Gemäß Art. 2 Abs. 1 ist die DSGVO sachlich anwendbar, sofern

1. personenbezogene Daten ganz oder teilweise automatisiert verarbeitet werden (Alt. 1) oder
2. zwar keine automatisierte Verarbeitung erfolgt, aber Daten verarbeitet werden, die in einem „Dateisystem“ gespeichert sind oder gespeichert werden sollen (Alt. 2).

Art. 2 Abs. 2 DSGVO regelt Ausnahmen von dem durch Abs. 1 vorgegebenen sachlichen Anwendungsbereich, wobei für den Bereich des Online-Datenschutzes vor allem die sog. „**Haushaltsausnahme**“ Bedeutung hat, nach welcher die DSGVO keine Anwendung findet auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Bei den vorliegend relevanten **Online-Sachverhalten**, also Datenverarbeitungen im Zusammenhang mit Websites und Apps, liegt stets auch eine ganz oder teilweise automatisierte Datenverarbeitung vor. Soweit Websites und Apps für unternehmerische Zwecke oder Zwecke eines Vereins eingesetzt werden, kommt auch ein Eingreifen der Haushaltsausnahme nicht in Betracht.



¹⁷ DSK (Hg.): Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1, Rn. 20 ff., online: https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf [30.01.24].

Entscheidend für die Einschlägigkeit der DSGVO auf Online-Sachverhalte ist damit, inwiefern im Zusammenhang mit Websites und Apps personenbezogene Daten von Nutzern verarbeitet werden. Personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen [...]“ (nach Legaldefinition in Art. 4 Nr. 1 DSGVO).

Informationen in diesem Sinne können etwa Name, Geschlecht, Kontoverbindung, Adresse oder Bestellinformationen im Rahmen des Onlineshopping sein, über Messengerdienste ausgetauschte Nachrichten (Kommunikations- und Inhaltsdaten) oder sonstige Spuren, die Nutzer im Netz hinterlassen.

Sind IP-Adressen und Cookies **PERSONENBEZOGENE DATEN** mit der Folge, dass bei deren Verarbeitung die DSGVO zu beachten ist?

Auf der Grundlage von Vorgaben des EuGH* hat der BGH** entschieden, dass die **dynamische IP-Adresse** (diese werden immer wieder neu vergeben) für den Webseitenbetreiber ein personenbezogenes Datum darstellen kann. Aus dieser Rechtsprechung kann zwar nicht der Schluss gezogen werden, jede (dynamische) IP-Adresse sei stets ein personenbezogenes Datum. Es gibt genügend Fälle, in denen die Zuordnung zu einer natürlichen Person nicht möglich ist, z. B. bei Nutzung von Internetcafés oder offenen WLANS ohne Registrierungspflicht. Die theoretisch mögliche Unterscheidung zwischen personenbezogenen und nichtpersonenbezogenen IP-Adressen ist für die Praxis allerdings zumeist ohne Konsequenz. Wenn nämlich im konkreten Anwendungsszenario nicht sicher ausgeschlossen werden kann, dass ein Pool von IP-Adressen auch personenbeziehbar Adressen enthält, sind im Ergebnis **alle IP-Adressen als personenbezogen zu behandeln**.

Cookies an sich bzw. über den Einsatz von Cookies gesammelte Datensätze weisen für sich betrachtet zunächst keinen Personenbezug auf. Denn selbst wenn Cookies eine eindeutige Kennung enthalten, was nicht der Fall sein muss, bedeutet dies nicht ohne Weiteres, dass auch eine Zuordnung der Kennungen zu konkreten natürlichen Personen möglich ist. Hat der Nutzer aber beim Anbieter zu einem früheren Zeitpunkt Identifikationsmerkmale hinterlassen oder hinterlässt er solche zu einem späteren Zeitpunkt, z. B. im Rahmen eines Bestell- oder Registrierungsvorgangs, ist ein entsprechender Personenbezug der Informationen gegeben.***

* EuGH, Ur. v. 19.10.2016 – C-582/14 (Rechtssache Breyer), Rn. 38 ff.

** BGH, Ur. v. 16.5.2017 – VI ZR 135/13.

*** Klar/Kühling in Kühling/Buchner DS-GVO/BDSG Art. 4 Nr. 1 Rn. 36.



b) Anforderungen der DSGVO an (Online-) Datenverarbeitungen und Verhältnis von DSGVO und TTDSG

Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, müssen diese entweder mit Einwilligung der betroffenen Person oder auf Basis einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden (vgl. Erwägungsgrund 40 DSGVO).

Als sonstige Rechtsgrundlagen im vorgenannten Sinne kommen insbesondere Art. 6 Abs. 1 lit. b und f DSGVO in Betracht. Die erstgenannte Norm ermöglicht erforderliche personenbezogene Datenverarbeitungen im Zusammenhang mit Verträgen und bestimmten Konstellationen mit den betroffenen Personen. Die letztgenannte Bestimmung gestattet Verarbeitungen zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person das Verarbeitungsinteresse überwiegen.

Wie bereits ausgeführt, kommen § 25 TTDSG und die DSGVO-Bestimmungen nebeneinander zur Anwendung, soweit mit dem Zugriff auf ein Endgerät eine personenbezogene Datenverarbeitung einhergeht.



Im Hinblick auf das Zusammenspiel der beiden Regelungskomplexe können folgende Grundsätze zusammengefasst werden:*

Werden im Rahmen des Zugriffs auf die Endeinrichtung personenbezogene Daten verarbeitet, wird regelmäßig, wenn die Vorgaben von § 25 Abs. 2 TTDSG eingehalten sind, auch ein DSGVO-Zulässigkeitstatbestand einschlägig sein, regelmäßig Art. 6 Abs. 1 Buchst. b DSGVO (Vertrag) oder Art. 6 Abs. 1 Buchst. f DSGVO (sog. Interessenabwägung). Bedarf es nach § 25 TTDSG der Einwilligung, so kann diese die personenbezogene Datenverarbeitung mitabdecken.

Wichtig ist, dass dies andersherum nicht der Fall ist: Allein der Umstand, dass eine mit dem Endgerätezugriff verbundene Datenverarbeitung nach Art. 6 DSGVO legitimierbar ist, bedeutet nicht, dass auch eine Zulässigkeit nach § 25 TTDSG anzunehmen ist.

* Vgl. Schwartmann/Reif/Burkhardt in Schwartmann/Jaspers/Eckhardt: TTDSG, § 25 Rn. 152 f.

So darf nach Erwägungsgrund 47 S. 7 DSGVO eine Verarbeitung personenbezogener Daten zum Zwecke der **Direktwerbung** grundsätzlich als „eine einem berechtigten Interesse dienende Verarbeitung“ betrachtet werden. Werbliche Datenverarbeitungen können also im Grundsatz über eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO legitimiert werden.¹⁸ Endgerätzugriffe zu Werbezwecken, insbes. **Werbe-Cookies**, sind jedoch nach § 25 TTDSG einwilligungsbedürftig (vgl. hier im Abschnitt „Anforderungen an Cookies und Co.“ ab S. 9). Der Endgeräteschutz nach TTDSG kennt anders als die DSGVO keine Interessenabwägung.

3. Datenschutzerklärung

Ein zentraler Grundsatz der DSGVO ist das Erfordernis der **Transparenz der personenbezogenen Datenverarbeitung** (Art. 5 Abs. 1 lit. a DSGVO). Die von der Verarbeitung betroffene Person, hier der Internetnutzer, soll nachvollziehen können, wer die Daten zu welchen Zwecken verarbeitet. Hinsichtlich der Datenverarbeitungen im Zusammenhang mit einer Webseite ist dies dadurch gewährleistet, dass der Anbieter auf seiner Seite Informationen zum Datenschutz zur Verfügung zu stellen hat (die sogenannte „**Datenschutzerklärung**“). Die konkrete Verpflichtung, solche Informationen vorzuhalten, ergibt sich aus Art. 13 DSGVO, der die Informationspflichten bei Erhebung personenbezogener Daten bei der betroffenen Person regelt.

Ein allgemeingültiges Muster für eine solche Erklärung kann es nicht geben, denn Webseiten weisen unterschiedliche Funktionalitäten auf und haben in der Folge über unterschiedliche Datenverarbeitungen zu informieren.

In der Praxis stellen Webseitenbetreiber in der „Datenschutzerklärung“ teilweise auch Informationen zu ihren sonstigen, nicht im Zusammenhang mit dem Internetauftritt stehenden Datenverarbeitungen zur Verfügung. Hierbei handelt es sich um freiwillige Informationen.



¹⁸ Es besteht allerdings ein Widerspruchsrecht des Betroffenen, auf das dieser auch hinzuweisen ist (vgl. Art. 21 Abs. 2 und 4 DSGVO).

a) Grundprinzipien bei Erstellung der Datenschutzerklärung



Bei Erstellung der Datenschutzerklärung für Onlineangebote, wie z. B. Websites und Apps, sollten folgende allgemeine Grundsätze beachtet werden:

1. **Weniger ist mehr:** Eine knappe, aber trotzdem verständliche Information über die auf der Internetseite durchgeführten Endgerätzugriffe Datenverarbeitung ist wirkungsvoller als allgemeine Ausführungen.
2. **Gliederung nutzen:** Gerade bei komplexer gestalteten Onlineangeboten, z. B. bei eingebundenen Diensten Dritter und/oder der Verfolgung diverser Verarbeitungs- bzw. Zugriffszwecke, kann eine Gliederung der Datenschutzerklärung für zusätzlichen Überblick sorgen und dem Nutzer helfen, relevante Informationen schnell aufzufinden.
3. **Werbung mit Selbstverständlichkeiten vermeiden:** Die Einhaltung der Datenschutzvorschriften ist eine Selbstverständlichkeit. Gesetzes-treues Verhalten sollte nicht besonders herausgestellt werden.
4. Mittels der Datenschutzerklärung werden Transparenzpflichten erfüllt. Die Datenschutzerklärung ist nicht der geeignete Ort, um eine Legitimation ansonsten nicht erlaubter Datenverarbeitungen bzw. Endgerätzugriffe herbeizuführen. Die Einholung ggf. notwendiger **Einwilligungen** erfolgt über das **Consent-Banner**.¹⁹
5. Die Datenschutzerklärung **bedarf keiner Zustimmung** des Nutzers. Auch ist es nicht erforderlich, sich die Kenntnisnahme durch den Nutzer bestätigen zu lassen. Ausreichend, aber auch unabdingbar ist, dass über eine **Dokumentation** des Online-Angebots der Informationsprozess als solcher nachgewiesen werden kann.
6. Eine schnelle und unbürokratische Möglichkeit zur **Kontaktaufnahme bei Fragen zum Datenschutz** kann beim Nutzer Vertrauen schaffen. Ohnehin haben Verantwortliche nach Art. 37 Abs. 7 DSGVO die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Ein geeigneter Ort hierfür ist u. a. die Datenschutzerklärung auf der Homepage. Der/die Datenschutzbeauftragte muss nicht namentlich benannt werden, es genügt z. B. die Angabe einer (Funktions-)E-Mail-Adresse (z. B.: dsb@unternehmen.de).

¹⁹ Siehe Abschnitt „Cookie-/Consent-Banner“ ab S. 12.

b) Checkliste Datenschutzerklärung

Aufbau und formale Anforderungen	Check: Ja/Nein
----------------------------------	----------------

Von jeder Unterseite des Angebots mit einem Klick erreichbar ²⁰	
Präzise, transparente, verständliche und leicht zugängliche Form und Formulierung in klarer und einfacher Sprache	
Je nach Länge und Komplexität der Erklärung: Gliederung/Inhaltsverzeichnis voranstellen <ul style="list-style-type: none"> – ggf. Präambel/Einleitung – ggf. vorangestellter Unterabschnitt mit Definitionen von Begriffen wie Cookies, IP-Adressen etc. (alternativ: Erläuterung im Rahmen des jeweiligen Kontexts) 	
Datum der letzten Aktualisierung einstellen	
<i>Optional:</i> Downloadmöglichkeit der Datenschutzerklärung	
<i>Optional:</i> Archiv mit Vorgängerversionen (<i>Hinweis:</i> Jedenfalls intern bedarf es eines Versionsmanagements)	

Notwendige Basisinformationen (allgemein)	Check: Ja/Nein
---	----------------

Name und Kontaktdaten des Verantwortlichen (ggf. auch Vertreter gemäß Art. 27 DSGVO, z. B. des die Webseite betreibenden Unternehmens)	
Kontaktdaten des/der Datenschutzbeauftragten, soweit benannt (<i>Hinweis:</i> Die Angabe des Namens ist nicht notwendig; die Angabe einer Funktions-E-Mail-Adresse ist ausreichend)	

²⁰ Artikel-29-Gruppe: WP 260 rev.01. Leitlinien für Transparenz gemäß der Verordnung 2016/679, Rn. 11, online: <https://www.datenschutzkonferenz-online.de/wp29-leitlinien.html> [30.01.2024].

<p>Datenverarbeitungen (Log-Files) zur Bereitstellung des Online-Angebots, inklusive Rechtsgrundlage und unter Benennung der typischerweise anfallenden Informationen²¹</p> <p>(<i>Hinweis:</i> Die korrekte Rechtsgrundlage der Datenverarbeitung bei rein informatorischer²² Nutzung von Websites ist nicht abschließend geklärt.²³ Für die Praxis empfiehlt es sich, parallel auf Art. 6 Abs. 1 lit. b und/oder f DSGVO hinzuweisen)</p>	
<p>Empfänger oder Kategorien von Empfängern der personenbezogenen Daten benennen</p> <p>(<i>Hinweise:</i> Empfänger sind auch Auftragsverarbeiter, z. B. Webhostingdienstleister. Eine Übermittlung von Nutzerdaten an weitere Verantwortliche, z. B. Onlinemarketing-Anbieter, kommt nur bei Vorliegen eines entspr. Erlaubnistatbestand nach Art. 6 Abs. 1 DSGVO in Betracht.²⁴</p> <p>Nach dem EuGH²⁵ hat die betroffene Person iR von Auskunftsbeghehrs nach Art. 15 DSGVO Anspruch auf Offenlegung der konkreten Identität des Empfängers. Jedenfalls, wenn der Betroffene es anders verlangt, reicht es insoweit nicht mehr, bloß Kategorien von Empfängern, z. B. nach Branchenzugehörigkeit, zu benennen.</p> <p>Nicht abschließend geklärt sind die Auswirkungen der EuGH-Entscheidung für Informationen nach Art. 13 DSGVO. Im Hinblick auf die unterschiedlichen Zwecke von Art. 13 und 15 DSGVO wird vertreten, i. R. v. Art. 13 Abs. 1 lit. e DSGVO bestehe nach wie vor ein Wahlrecht, nur Kategorien von Empfängern zu benennen.)</p>	

21 IP-Adresse, Datum und Uhrzeit der Anfrage, Zeitzonendifferenz zur Greenwich Mean Time (GMT), Inhalt der Anforderung (besuchte Seite), Zugriffsstatus/HTTP-Statuscode, jeweils übertragene Datenmenge, vorher besuchte Seite, Browser, Betriebssystem, Sprache und Version der Browsersoftware, vgl. Ansgar Koreng/Matthias Lachenmann: DatenschutzR-FormHdB, Form. F. I. 1. Anm. 1.–15., online: https://beck-online.beck.de/Dokument?vpath=bibdata%2Fform%2FKorengLachenmannFbDSR_3%2Fcont%2FKorengLachenmannFbDSR.Inhaltsverzeichnis.htm&anchor=Y-600-W-KORENGLACHENMANNFbDSR&jumpType=Jump&jumpWords=koreng&readable=Suche%2Bnach%2BFormularsammlung%253a%2BKoreng [11.01.2024].

22 Gemeint ist die bloße Betrachtung der Website, ohne dass etwa eine Registrierung erfolgt, vgl. ebd.

23 Vgl. ebd., Rn. 6.

24 Vgl. ebd., Rn. 8.

25 Urteil des Gerichtshofs vom 12.1.2023, Rechtssache C-154/21, online: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=269146&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1> [30.01.2024].

<p>Benennen von Speicherdauer bzw. Kriterien für die Festlegung derselben bezogen auf</p> <ul style="list-style-type: none"> – Webserver-Log-Files – ggf., sofern eingesetzt, Cookies <p>(<i>Hinweis:</i> Die zulässige Laufzeit von Cookies ist abhängig von deren Zweck. Soweit dies zur Zweckerreichung genügt, sind Cookies nach Ablauf der Sitzung („Session“) zu löschen.</p> <p>Dauerhafte, sog. persistente Cookies, bedürfen regelmäßig einer Einwilligung des Nutzers. Dies gilt insbes. für Werbe-Cookies.)</p>	
<p>Benennen des Bestehens der Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit</p>	
<p>Benennen des Bestehens eines Beschwerderechts bei einer Aufsichtsbehörde</p>	

Sofern zutreffend, zusätzliche Informationen erforderlich bzgl.:

Check: Ja/Nein

<p>Im Fall eines beabsichtigten Drittlandtransfers von Daten bedarf es zusätzlich folgender Informationen, z. B. bei Verwendung von Social Media Plugins und der Einbindung von Google Diensten:</p> <p>Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gem. Art. 46 oder Art. 47 oder Art. 49 Abs. 1 Unterabsatz 2 DSGVO einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.</p>	
<p>Im Fall einwilligungsbasierter Datenverarbeitung:</p> <p>Hinweis auf das Recht, die Einwilligung jederzeit widerrufen zu können, ohne dass die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird.</p> <p>(<i>Hinweis:</i> Da der Widerruf der Einwilligung so leicht sein soll wie deren Erteilung,²⁶ sollte ein Widerruf nicht nur über die Datenschutzerklärung ermöglicht werden, sondern bereits auf der Startseite des Online-Angebots, z. B. über einen Link im Footer der Seite möglich sein.)</p>	

²⁶ Art. 7 Abs. 3 S. 4 DSGVO.

<p>In Fällen automatisierter Entscheidungsfindung einschließl. Profiling²⁷:</p> <ul style="list-style-type: none"> – Umstand der automatisierten Entscheidungsfindung einschließl. Profiling – aussagekräftige Informationen über die involvierte Logik sowie Tragweite und Auswirkungen für die betroffene Person 	
---	--

Je nach Ausgestaltung des konkreten Online-Angebots ist ggf. über Datenverarbeitungen bzw. Endgerätzugriffe zu weiteren Zwecken zu informieren, z. B.:

Check: Ja/Nein

<p>Registrierungs- und Login-Prozess <i>Rechtsgrundlage Datenverarbeitung:</i> Ggf. Art. 6 Abs. 1 S. 1 lit. b DSGVO, ansonsten regelmäßig Art. 6 Abs. 1 S. 1 lit. f DSGVO <i>Rechtsgrundlage Endgerätzugriffe:</i> § 25 Abs. 2 Nr. 2 TTDSG, sofern erforderlich für die Erbringung des konkreten Onlinedienstes</p>	
<p>Authentifizierungs-Cookies für die Dauer der Sitzung²⁸ <i>Rechtsgrundlage:</i> § 25 Abs. 2 Nr. 2 TTDSG (i. V. m. Art. 6 Abs. 1 lit. b oder f DSGVO)</p>	
<p>Verarbeitung von Informationen zu Online-Bestellungen, wie z. B. Versandadresse, Informationen zum bestellten Produkt, Zahlungsinformationen <i>Rechtsgrundlage:</i> Art. 6 Abs. 1 S. 1 lit. b DSGVO</p>	
<p>Warenkorbcookies²⁹ <i>Rechtsgrundlage:</i> § 25 Abs. 2 Nr. 2 TTDSG (i. V. m. Art. 6 Abs. 1 lit. b oder f DSGVO)</p>	
<p>Bonitätsprüfung, z. B. bei Online-Shops <i>Rechtsgrundlage:</i> Art. 6 Abs. 1 S. 1 lit. f DSGVO</p>	
<p>Datenverarbeitung im Zusammenhang mit einem Kontaktformular <i>Rechtsgrundlage:</i> Art. 6 Abs. 1 S. 1 lit. f DSGVO</p>	

²⁷ Art. 22 Abs. 1 und 4 DSGVO.

²⁸ Die dauerhafte Speicherung beim Nutzer setzt dessen Einwilligung voraus.

²⁹ Die zulässige Laufzeit solcher Cookies ist umstritten. Nach Ansicht der Datenschutzaufsichtsbehörden sollen diese allenfalls kurze Zeit, d. h. wenige Stunden, nach dem Schließen der Seite gespeichert werden dürfen.

<p>Einsatz von Tools zur Reichweitenmessung, d.h. zur statistischen Auswertung der Nutzung der Website (Tracking)</p> <p><i>Rechtsgrundlage Datenverarbeitung:</i> Art. 6 Abs. 1 S. 1 lit. f DSGVO oder Einwilligung</p> <p><i>Rechtsgrundlage Endgerätzugriffe:</i> § 25 Abs. 2 Nr. 2 TTDSG (str.)³⁰ bzw. Einwilligung</p>	
<p>Interessengerechte Anzeige von Werbung basierend auf vorangegangenem Nutzerverhalten (Targeting)</p> <p><i>Rechtsgrundlage Datenverarbeitung:</i> ggf. Art. 6 Abs. 1 S. 1 lit. f DSGVO, ansonsten Einwilligung</p> <p><i>Rechtsgrundlage Endgerätzugriffe:</i> Einwilligung</p>	
<p>Einbindung von Social Media Plug-ins von Facebook, Twitter, Instagram und Co. (mittels Zwei-Klick-Lösung bzw. Shariff³¹)</p> <p><i>Rechtsgrundlage:</i> Einwilligung</p>	
<p>Einbindung von Kartendiensten wie Google Maps (mittels Zwei-Klick-Lösung bzw. Shariff)</p> <p><i>Rechtsgrundlage:</i> Einwilligung</p>	
<p>Einsatz von Webfonts wie z. B. Google Fonts</p> <p>Prüfung im Einzelfall, notfalls Verzicht und nur lokale Einbindung von Fonts (alternativ: Einwilligung des Nutzers)</p>	
<p>Zahlungsabwicklung, ggf. unter Einsatz von externen Dienstleistern</p> <p><i>Rechtsgrundlage:</i> Art. 6 Abs. 1 S. 1 lit. b oder f DSGVO</p>	
<p>Newsletter Registrierung</p> <p><i>Rechtsgrundlage:</i> Einwilligung</p>	
<p>Sonstige Zwecke (konkret benennen)</p> <ul style="list-style-type: none"> – Angabe der Rechtsgrundlage der Datenverarbeitung und/oder des Endgerätzugriffs – <u>Sofern zutreffend:</u> Verpflichtung oder Obliegenheit zur Bereitstellung der Daten – Sofern Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (Interessenabwägung): Angabe der verfolgten berechtigten Interessen 	

³⁰ Vgl. im Einzelnen Schwartmann/Reif/Burkhardt in Schwartmann/Jaspers/Eckhardt: TTDSG, § 25 Rn. 143 ff.

³¹ Bernd Behr: Shariff – Social-Media-Buttons mit Datenschutz, in: c't Magazin online, 27.11.2014, online: <https://www.heise.de/hintergrund/Ein-Shariff-fuer-mehr-Datenschutz-2467514.html> [11.01.2024].

III. Sammlung weiterführender Links

Bezeichnung	Link
RL 2009/136	https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32009L0136
TTDSG	https://www.gesetze-im-internet.de/ttdsg/TTDSG.pdf
DSGVO	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
DSK Orientierungshilfe für Telemedienanbieter:innen Stand Dez. 2022	https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf
Auswertungsbericht der DSK zur Orientierungshilfe für Telemedienanbieter:innen	https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Auswertung_Konsultation_zur_Orientierungshilfe_fuer_Anbieter_von_Telemedien_final.pdf
LfD Niedersachsen: Hinweise zur Einwilligung	https://lfid.niedersachsen.de/download/161158
IHK München zu rechtssicheren Webseiten	https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Internetrecht/Rechtssichere-Internetseite/
IHK Wiesbaden zu rechtssicheren Webseiten	https://www.ihk.de/wiesbaden/recht/rechtsberatung/internetrecht-und-werbung/internetauftritt-rechtliche-anforderungen-und-pflichten-125572
Online-Publikation der AWV: DSGVO für kleine und mittlere Unternehmen Stand 2022	https://www.awv-net.de/dsgvo-kmu





Über den AWW-Arbeitskreis „Datenschutz und Informationssicherheit“

Mangelndes Vertrauen hinsichtlich des Schutzes der persönlichen Daten im Internet ist der Hauptgrund für die Nutzer, Geschäfte nicht online abzuwickeln. Datenschutz und Datensicherheit sind dementsprechend Themen, die dauerhaft eine hohe Priorität besitzen und ein verstärktes Interesse bei Bürgern und Politikern, Arbeitnehmern, Kunden und Datenschützern hervorrufen.

Einer der Themenschwerpunkte des Arbeitskreises ist die europäische Datenschutz-Grundverordnung. Die mit der vorgelegten Verordnung verfolgte Zielsetzung, den Datenschutz in Europa zu modernisieren und zu harmonisieren, wird ausdrücklich begrüßt. Dies gilt insbesondere für das Bestreben, bürokratische Regelungen abzubauen und das Datenschutzrecht zu vereinfachen, ohne dessen Zielsetzung einzuschränken. Weitere Themen, über die diskutiert werden, sind z. B. die datenschutzrechtlichen Aspekte beim Cloud-Computing, dem Einsatz KI, die Entwicklungen im Drittstaatentransfer und die Diskussionen um ein Beschäftigtendatenschutzgesetz. Auch Stellungnahmen zu nationalen und europäischen Gesetzesvorhaben werden vom Arbeitskreis erarbeitet.

Durch den regelmäßigen Informationsaustausch mit dem Bundesministerium des Innern und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie den Aufsichtsbehörden ist gewährleistet, dass der Arbeitskreis aktuell informiert ist und praktische Erfahrungen aus den Unternehmen an den Gesetzgeber und die Verwaltung herangebracht werden. Von Seiten der Wirtschaft sind Datenschutzbeauftragte von Unternehmen im Arbeitskreis vertreten.

Arbeitskreisleiter ist Rudi Kramer (DATEV eG, Nürnberg). Stellvertretende Arbeitskreisleitung sind Wulf Hartmann (Bundesverband deutscher Banken e.V., Berlin) und Kei-Lin Ting-Winarto (Deutscher Industrie- und Handelskammer, Berlin).



Gefördert durch:



aufgrund eines Beschlusses
des Deutschen Bundestages