Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

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

Websites rechtskonform gestalten

Die Bedeutung von 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 „Datenschutz und Informationssicherheit“, 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

2. Auflage überarbeitet von:
Rudi Kramer, Nürnberg (Leiter des AWV-Arbeitskreises 4.3)
Yvette Reif, Bonn

Genderhinweis: Aus Gründen der leichteren Lesbarkeit wird in dieser Publikation nicht ausdrücklich in geschlechtsspezifische 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. I Nicole Wingender, AWV e.V.
Layout und Satz: Cora Strasdat, AWV e.V.
Bildquellennachweis Cover: Adobe Stock/pla2na
Eschborn, 2., überarbeitete Auflage, Oktober 2025
AWV-Best.-Nr.: 43241-w

Hinweis

Diese Handreichung ist ein Leitfaden für Betreiber von Websites, insbesondere kleine und mittlere Unternehmen (KMU), welche über ein Grundlagenwissen im Themenbereich Datenschutzrecht verfügen. Weiterführende Informationen zum Thema Datenschutz liefert beispielsweise die im Jahr 2022 veröffentlichte Broschüre „Die DSGVO – Informationen für kleine und mittlere Unternehmen“ des AWV-Arbeitskreises „Datenschutz und Informationssicherheit“.

Seit der 1. Auflage dieser Handreichung im Jahr 2024 hat der nationale Gesetzgeber mit Blick auf die Harmonisierung des europäischen Binnenmarktes den deutschen Begriff des „Telemediums“ durch denjenigen des „digitalen Dienstes“ ersetzt und das frühere „Telekommunikation-Telemedien-Datenschutzgesetz (TTDSG)“ umbenannt in „Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)“.

Die Neuauflage dieses Papiers erfolgt v. a. vor dem Hintergrund, die Ausführungen an die aktuell geltenden gesetzlichen Begriffsbestimmungen sowie die zwischenzeitlich ergangene Rechtsprechung anzupassen. Zentrale inhaltliche Änderungen gehen mit der Neuauflage nicht einher.

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

www.awv-net.de/dsgvo-kmu

AWV-Arbeitskreis 4.3 „Datenschutz und Informationssicherheit“

Eschborn im Oktober 2025

Inhalt

I. Datenschutzrechtliche Anforderungen bei Onlineauftritten und der Einbindung von Cookies

Bei der Gestaltung von Websites sind diverse rechtliche Anforderungen zu beachten. Die vorliegende Handreichung konzentriert sich auf die datenschutzrechtlichen Anforderungen sowie die an den Schutz der Privatsphäre bei der Nutzung von Endgeräten (ePrivacy).

Basis der Anforderungen mit Blick auf die ePrivacy sind Vorgaben, die sich aus einer europäischen Richtlinie aus dem Jahr 2002[1] (ePrivacy-Richtlinie) ergeben und die im Jahr 2009[2] nochmal auf europäischer Ebene konkretisiert wurden (sog. Cookie-Richtlinie). Sachlicher Gegenstand der angesprochenen 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 Grundrechtcharta[3] geschützt.

Die Grundrechtecharta ist jedoch nur für die Organe der europäischen Gemeinschaft bindend und europäische Richtlinien müssen zu ihrer Wirksamkeit auf nationaler Ebene zunächst 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 an umstritten, ob diese Umsetzung in Deutschland ausreichend erfolgte. Diese Diskussion versuchte der Gesetzgeber mit Erlass des Telekommunikation-Telemedien-Datenschutzgesetzes (TTDSG) zu beenden, das zum 1. Dezember 2021 in Kraft trat. Im TTDSG wurden Regelungssachverhalte aus dem TKG und TMG zusammengeführt und teilweise neu formuliert.

Im Zusammenhang mit der Durchführung des europäischen „Digital Services Act“ (DSA) wurde in Deutschland in der Folge aber der nationale Begriff des Telemediums aufgegeben und durch den europäischen Begriff des „digitalen Dienstes“ ersetzt, da vor dem Hintergrund der harmonisierten europäischen Vorschriften für einen Binnenmarkt für digitale Dienste kein Raum für den rein national vorgeprägten Begriff des Telemediums blieb.[4] Im Mai 2024 wurde das TTDSG daher umbenannt in „Telekommunikation-

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 Grundrechtecharta 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.“

4 BT-Drs. 20/10031, S. 67.

Digitale-Dienste-Datenschutz-Gesetz – TDDDG“. Außerdem wurden die Begrifflichkeiten innerhalb des Gesetzes an die neue Terminologie angepasst.

Werden bei der Bereitstellung und Nutzung von digitalen Diensten Informationen verarbeitet, die personenbeziehbar sind, gelten zusätzlich die Anforderungen, die sich aus der Datenschutz-Grundverordnung (DSGVO)[5] ergeben. Zu dieser hat die AWV bereits eine Broschüre veröffentlicht.[6]

Wird etwa im Rahmen der Erstellung bzw. des Betreibens der Website 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 Website in diesem Sinne im Auftrag[7], ist mit diesem eine Vereinbarung zur Umsetzung der Anforderungen an eine Auftragsverarbeitung nach den Vorgaben des Art. 28 DSGVO abzuschließen. Auch hierzu informiert die bereits erwähnte AWV-Publikation zur DSGVO. Bezüglich der Websiteerstellung sollte vertraglich fixiert werden, welche Datenfelder mit Personenbezug erstellt werden und welche Cookies oder vergleichbare technische Maßnahmen für welchen Zweck eingesetzt werden sollen.

Daneben gibt es bei Websites weitere Pflichten, insbesondere Informationspflichten, die sich z. B. 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 den Industrie- und Handelskammern.[8] Beachten Sie dabei, dass inzwischen die Vorgaben des § 5 TMG zur Impressumspflicht in § 5 Digitale-Dienste-Gesetz (DDG) überführt wurden.

5 European Union (Hg.): EUR-lex. Access to European Union law, online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [27.06.2025].

6 AWV (Hg.), Die DSGVO – Hinweise für kleine und mittlere Unternehmen, 2022, https://www.awv-net.de/publikationen-produkte/publikationen/detailseite/die-dsgvo-hinweise-fuer-kleine-und-mittlere-unternehmen [27.6.2025].

7 Der zivilrechtliche Begriff des Auftrags ist insofern nicht entscheidend. Ein Unternehmer kann also zivilrechtlich Auftragnehmer sein, ohne auch datenschutzrechtlich Auftragsverarbeiter zu sein.

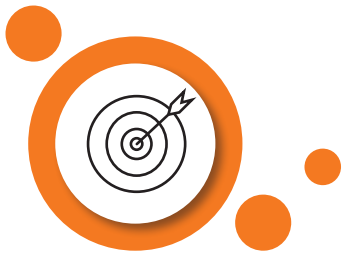
8 Vgl. bspw. Industrie- und Handelskammer Wiesbaden (Hg.): Rechtliche Pflichten für Websites – Impressum, Datenschutz etc., online: https://www.ihk.de/wiesbaden/recht/rechtsberatung/internetrecht-und-werbung/internetauftritt-rechtliche-anforderungen-und-pflichten-1255572 [27.06.2025].

II. Die Anforderungen an Websitebetreiber im Einzelnen

Betreiber von Websites, Apps und Co. haben die Vorgaben des TDDDG, insbes. § 25 TDDDG, 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 deren sachlicher Anwendungsbereich. Zudem wird der Rechtsrahmen dargestellt, der sich aus § 25 TDDDG 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-Digitale-Dienste-Datenschutz-Gesetz (TDDDG)

a) Anwendungsbereich des TDDDG



Das TDDDG enthält „besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und digitalen Diensten“, vgl. § 1 Abs. 1 Nr. 2 TDDDG. Anbieter von digitalen Diensten ist nach § 2 Abs. 2 Nr. 1 TDDDG „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“. Beispiele für Telekommunikationsdienste sind neben traditioneller Sprachtelefonie, Textmitteilungs- und E-Mail-Diensten u. a. auch das Angebot von Internettelefonie, Messengerdiensten oder webgestützten E-Mail-Diensten.

Bzgl. des Begriffs des „digitalen Dienstes“ verweist das TDDDG in § 2 Abs. 1 auf das Digitale-Dienste-Gesetz (DDG). Nach § 1 Abs. 4 Nr. 1 DDG ist ein **digitaler Dienst** „ein Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1)“. Im letztgenannten Sinne meint „Dienst“ „eine Dienstleistung der Informationsgesellschaft, d. h., jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung“. Diese im Ergebnis maßgebliche Definition des digitalen Dienstes ist insofern bemerkenswert, als hiervon nur solche Dienstleistungen der Informationsgesellschaft erfasst sind, die **regelmäßig entgeltpflichtig** sind.

Der Begriff des digitalen Dienstes ist damit nicht deckungsgleich mit dem Vorgängerbegriff des Telemediums, denn für das Vorliegen eines Telemediums sollte es gerade nicht entscheidend sein, ob für die Nutzung des Dienstes ein Entgelt erhoben wird (vgl. § 1 Abs. 1 S. 2 Telemediengesetz a. F.). Websites und Apps bildeten insofern das klassische Anwendungsszenario für ein Telemedium.

Mit Blick auf die geänderte Definition erscheint fraglich, ob bereits „einfache" Websites zur Information über ein Unternehmen bzw. eine öffentliche Stelle den Begriff des digitalen Dienstes erfüllen.[9]

Bezogen auf die hier relevante Frage der Einwilligungsbedürftigkeit von Cookies & Co., die im Zusammenhang mit dem Angebot von Websites und Apps zum Einsatz kommen, dürfte der Änderung mit Blick auf die Begrifflichkeiten jedoch im Ergebnis keine Konsequenz zukommen. Denn Abs. 1 des insoweit maßgeblichen § 25 TDDDG bezieht sich gar nicht auf digitale Dienste, sondern besagt ganz allgemein, dass „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind" im Ausgangspunkt der Einwilligung des Nutzers bedarf. Diese tatbestandlichen Voraussetzungen sind aber auch erfüllt, wenn Anbieter „einfacher" Informationswebsites Cookies oder vergleichbare Techniken einsetzen. Auf das Vorliegen eines digitalen Dienstes ist nur in § 25 Abs. 2 Nr. 2 TDDDG abgestellt, wonach Zugriffe auf Endeinrichtungen ausnahmsweise dann nicht der Einwilligung bedürfen, wenn diese „unbedingt erforderlich" sind, „damit der Anbieter eines digitalen Dienstes einen vom Nutzer ausdrücklich gewünschten digitalen Dienst zur Verfügung stellen kann". Auf diese Bestimmung dürften sich Anbieter „einfacher" Websites jedenfalls entsprechend berufen dürfen. Es ist nicht davon auszugehen, dass sie mit Blick auf den Einsatz von Cookies und vergleichbaren Verfahren stärker reguliert werden sollen als Anbieter entgeltpflichtiger Angebote.

9 Amélie Heldt, Sarah Legner (Hg.): Digitale-Dienste-Gesetz: DDG, (2025), § 1 Rn. 20. Irritierend erscheint insofern der Hinweis in der Gesetzesbegründung, dass der sachliche Anwendungsbereich des Begriffs Telemedium gänzlich in der neuen Terminologie aufgehe und sich inhaltliche Änderungen durch die Umbenennung nicht ergeben sollen (vgl. BT-Drs. 20/10031, S. 92).

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.

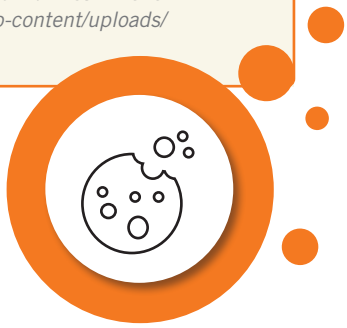
Was sind COOKIES?*

Cookies sind kleine Datensätze, die der Webbrowser auf dem Endgerät speichert. Anhand von Cookies erkennt eine Website, wer sie gerade besucht, so dass etwa Nutzereingaben wie Sprach- oder Login-Informationen nicht immer wieder erneut getätigt werden müssen. 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.

Mit Blick auf die Speicherdauer gibt es einerseits sog. **persistente Cookies**, die dauerhaft bzw. für eine bestimmte Laufzeit im System des Nutzers hinterlegt werden, andererseits sog. **Session Cookies**, die gelöscht werden, 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 TDDDG das Setzen und Auslesen von Cookies bzw. vergleichbare Verfahren im Ausgangspunkt an eine vorherige Einwilligung des Nutzers. Von diesem grundsätzlichen Einwilligungserfordernis sind nach § 25 Abs. 2 TDDDG lediglich zwei Ausnahmen vorgesehen. Praxisrelevant ist v. a. die zweite in § 25 Abs. 2 TDDDG vorgesehene Ausnahme:[10]

10 Die Ausnahme nach § 25 Abs. 2 Nr. 1 TDDDG erlangt Bedeutung im Fall der Nachrichtenübertragung. Die Regelung hat folgenden Inhalt: „Die Einwilligung nach Absatz 1 ist nicht erforderlich, wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist."

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

Als **einwilligungsfrei möglich** werden etwa nachfolgende Kategorien von Cookies angesehen, sofern die **Cookies** nicht für weitere Zwecke verwendet werden:[11]

- **User-Input-Cookies (Session-ID)**
  Darunter sind Cookies zu verstehen, die der einheitlichen Nachverfolgung von Nutzereingaben bei einer Reihe von Nachrichtenaustauschvorgängen mit einem Dienstleister dienen (z. B. Warenkorb-Cookies). Die Laufzeit solcher Cookies ist regelmäßig auf die Dauer der Sitzung beschränkt bzw. ggf. wenige Stunden hierüber hinaus.

- **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.

- **Cookies zur Anpassung der Benutzeroberfläche**
  Solche Cookies werden verwendet, um nicht mit einer anderen, dauerhaften Kennung (z. B. einem Benutzernamen) verknüpfte Einstellungen (z. B. Einstellung zur Sprache) für einen mehrere Unterseiten umfassenden Dienst zu speichern.

11 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.

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 das Ausspielen interessenbasierter Werbung steht in **keinem funktionalen Zusammenhang** zur Erbringung des digitalen Dienstes. Zwar mag es aus Sicht des Diensteanbieters zur Finanzierung seines Geschäftsmodells ggf. wirtschaftlich erforderlich sein, werbliche Zugriffe und anschließende Datenverarbeitungen durchzuführen. Eine bloß wirtschaftliche Erforderlichkeit ist im Rahmen von § 25 Abs. 2 Nr. 2 TDDDG 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 TDDDG sind, ist nicht abschließend geklärt. Nach Auffassung der französischen Datenschutzaufsichtsbehörde CNIL soll die § 25 Abs. 2 Nr. 2 TDDDG entsprechende Regelung in der europäischen ePrivacy-Richtlinie 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 ggf. 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: „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) sowie die spanische Aufsicht aepd, „Guía Uso de cookies para herramientas de medición de audiencia" (Januar 2024).*

** *Vgl. hierzu Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg: FAQ. Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps, Version 2.0.1 (März 2022), S. 13 ff.*

Schützt das TDDDG nur NATÜRLICHE PERSONEN?

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

Gehen mit dem Endgerätezugriff auch **personenbezogene Datenverarbeitungen** einher, kommen insoweit **§ 25 TDDDG 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-Datenverarbeitungen[12] – 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 TDDDG 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 TDDDG-Einwilligung ergibt sich dies über einen Verweis in § 25 Abs. 1 S. 2 TDDDG.

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.*

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

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 Punkte:

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

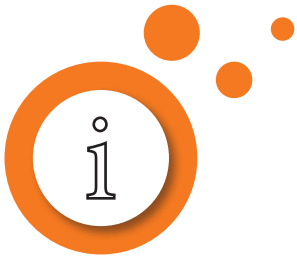
   - keine voreingestellten Ankreuzkästchen, aktive Handlung des Nutzers nötig („Planet49"-Entscheidung[13] des EuGH)
   - keine Einwilligung durch Weitersurfen
   - Beeinflussung der Nutzerentscheidung durch optische Gestaltung der Schaltflächen (sog. Nudging) ist nur zulässig, solange es „maßvoll" erfolgt
   - Möglichkeit zur Abwahl nicht erforderlicher Cookies muss regelmäßig bereits auf erster Bannerebene bestehen[14] (Insoweit existieren keine allgemeingültigen Gestaltungs- bzw. Formulierungsvorgaben. Nötig ist eine transparente und verständliche Gestaltung der Nutzerführung, bei welcher der Nutzer die erbetene Einwilligung auch ablehnen kann, ohne dass erheblicher Mehraufwand im Verhältnis zur Erteilung der Einwilligung entsteht.[15])

2. **Freiwilligkeit**

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

3. **Informiertheit**

   - Für wirksame Einwilligung nötige **Mindestinformationen:**[16]
     - Identität des Verantwortlichen
     - Zweck jedes Verarbeitungsvorgangs, für den die Einwilligung eingeholt wird



13 EuGH, Urt. v. 1.10.2019 – C-673/17.
14 BVwG Österreich 31.7.2024 – W108 2284491-1/15E; VG Hannover, 19.03.2025 – 10 A 5385/22; OLG Köln 19.1.2024 – 6 U80/23; LG München I 29.11.2022 – 33 O 14776/19.
15 VG Hannover, 19.03.2025 – 10 A 5385/22.
16 EDSA, Leitlinien 05/2020 zur Einwilligung gem. Verordnung 2016/679, Version 1.1, 04.05.2020, Rn. 64.

  - (Art der) Daten, die erhoben und verwendet werden
  - Hinweis auf das 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

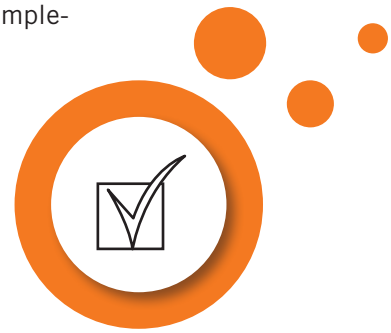
- Bei Einwilligungen in **Cookies zu Werbezwecken** gehören zu den **Mindestinformationen** auch:[17]
  - Angaben zur Funktionsdauer der Cookies
  - Angaben zu eventuellen Empfängern der in den Cookies enthaltenen Informationen

- Beachtung der **weitergehenden Informationspflichten** (Art. 13 f. DSGVO), u. a. mit Blick auf Empfänger der personenbezogenen Daten (z. B. Dienstleister)

- 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 Bannerebene befinden.

4. Nachweis der Einwilligung

- Nach Auffassung der nationalen Datenschutzkonferenz (DSK) genügt es, nachweisen zu können, dass und welche Prozesse implementiert wurden.



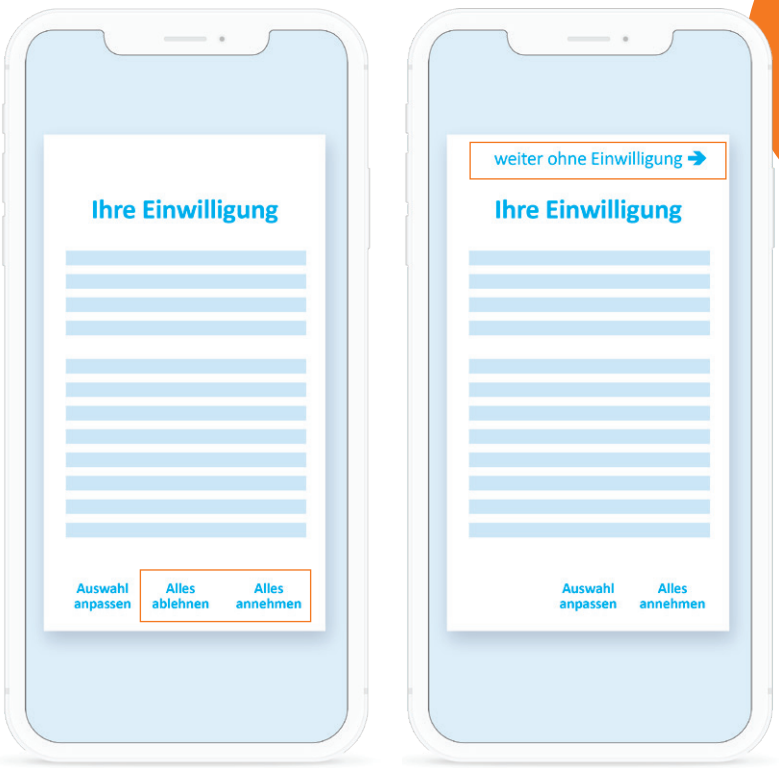
17 EuGH, Urt. v. 1.10.2019 – C-673/17 („Planet49“-Entscheidung).

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).
- Hinweispflicht bei Einholung der Einwilligung bzgl. Widerrufsrecht und dessen Rechtsfolgen

Siehe hierzu nachfolgende Beispiele:

Gestaltungsvorschläge der französischen Datenschutzaufsicht CNIL für Cookie-Banner*



* 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 [26.08.2025].

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 gegenüber dem Anbieter zu führen, können den Websitebetreiber aber im Verhältnis zur betroffenen Person bzw. zur Aufsichtsbehörde oder zu den 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 TDDDG auf Cookies vergleichbare Verfahren, z. B. sog. Browser- oder Device-Fingerprinting

§ 25 TDDDG 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 TDDDG 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.

Sofern vom Anbieter Programmcode auf dem Endgerät zur Ausführung gebracht wird, wie z. B. JavaScript, Flash oder Java, wird von einem sog. „aktiven Fingerprinting“ gesprochen. Aktives Fingerprinting bedarf nach § 25 TDDDG in jedem Fall einer Einwilligung. Ob auch „passives Fingerprinting“, bei dem zum Tracking nur Daten verwendet werden, die beim Aufruf des digitalen Dienstes ohnehin anfallen und automatisch an den An-

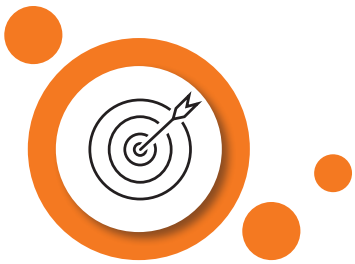
bieter übermittelt werden, einer Einwilligung nach TDDDG bedarf, ist strittig. Dieser Vorgang erforderte nach ursprünglicher Ansicht der DSK keine Einwilligung. In ihrer aktuellen Orientierungshilfe Digitale Dienste[18] trifft die DSK diese Aussage aber nicht mehr und es nicht auszuschließen, dass sich die DSK der insoweit abweichenden Position des EDSA anschließt.[19]

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 damit ein Eingreifen der Haushaltsausnahme nicht in Betracht.

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 […]“. (Legaldefinition in Art. 4 Nr. 1 DSGVO)

18 DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von digitalen Diensten (OH Digitale Dienste), Vers. 1.2..
19 EDSA, Guidelines 2/2023, Rn. 34 ff.

Informationen in diesem Sinne können etwa Name, Geschlecht, Kontoverbindung, Adresse oder Bestellinformationen im Rahmen des Onlineshoppings 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 wird vom TK-Anbieter bei jedem Einwahlvorgang neu vergeben) für den Websitebetreiber ein personenbezogenes Datum darstellen kann. Aus dieser Rechtsprechung kann zwar nicht der Schluss gezogen werden, dass jede dynamische IP-Adresse stets ein personenbezogenes Datum ist. 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 personenbeziehbare 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, Urt. v. 19.10.2016 – C-582/14 (Rechtssache Breyer), Rn. 38 ff.*
** *BGH, Urt. v. 16.5.2017 – VI ZR 135/13.*
*** *Klar/Kühling in Kühling/Buchner (Hg.): DS-GVO/BDSG Art. 4 Nr. 1 Rn. 36.*

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

Damit die Verarbeitung personenbezogener Daten rechtmäßig ist, muss diese entweder mit Einwilligung der betroffenen Person oder auf Basis einer sonstigen zulässigen Rechtsgrundlage erfolgen (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 zur Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der Person erfolgen. 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 TDDDG 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 TDDDG eingehalten sind, auch ein DSGVO-Zulässigkeitstatbestand einschlägig sein, regelmäßig Art. 6 Abs. 1 lit. b DSGVO (Vertrag) oder Art. 6 Abs. 1 lit. f DSGVO (sog. Interessenabwägung). Bedarf es nach § 25 TDDDG 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 TDDDG anzunehmen ist.

* *Vgl. Schwartmann/Reif/Burkhardt in Schwartmann/Jaspers/Eckhardt (Hg.): 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.[20] Endgerätzugriffe zu Werbezwecken, insbes. **Werbe-Cookies**, sind jedoch nach § 25 TDDDG einwilligungsbedürftig (vgl. hierzu den Abschnitt „Anforderungen an Cookies und Co." ab S. 9). Der Endgeräteschutz nach TDDDG 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 Website ist dies dadurch gewährleistet, dass der Anbieter auf seiner Site 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 Websites weisen unterschiedliche Funktionalitäten auf und haben in der Folge über unterschiedliche Datenverarbeitungen zu informieren.

Hinweis: In der Praxis stellen Websitebetreiber 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.

20 Es besteht allerdings ein Widerspruchsrecht der betroffenen Person, auf das diese 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 bzw. Datenverarbeitungen 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. Gesetzestreues 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**.[21]
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 Website. Der/die Datenschutzbeauftragte muss nicht namentlich benannt werden, es genügt z. B. die Angabe einer (Funktions-)E-Mail-Adresse (z. B.: dsb@unternehmen.de).

21 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[22]	
Präzise, transparente, verständliche und leicht zugängliche Form und Formulierung in klarer und einfacher Sprache	
Je nach Länge und Komplexität der Erklärung: Gliederung/Inhaltsverzeichnis voranstellen – 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	
Optional: Downloadmöglichkeit der Datenschutzerklärung	
Optional: Archiv mit Vorgängerversionen (*Hinweis:* Jedenfalls intern bedarf es eines Versionsmanagements)	

Notwendige Basisinformationen (allgemein)	Check: ja/nein
Name und Kontaktdaten des Verantwortlichen (regelmäßig die Stelle, welche die Website bzw. App betreibt) (ggf. auch Vertreter gemäß Art. 27 DSGVO)	
Kontaktdaten des/der Datenschutzbeauftragten, soweit benannt (Hinweis: Die Angabe des Namens ist nicht notwendig; die Angabe einer Funktions-E-Mail-Adresse ist ausreichend.)	

22 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 [26.08.2025].

Datenverarbeitungen zur Bereitstellung des Online-Angebots (Log-Files), inklusive Rechtsgrundlage und unter Benennung der typischerweise anfallenden Informationen[23]

(*Hinweis:* Die korrekte Rechtsgrundlage der Datenverarbeitung bei rein informatorischer[24] Nutzung von Websites ist nicht abschließend geklärt.[25] Für die Praxis empfiehlt es sich, parallel auf Art. 6 Abs. 1 lit. b und f DSGVO hinzuweisen.)

Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

(*Hinweise:* 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.[26]

Nach dem EuGH[27] hat die betroffene Person iR von Auskunftsbegehrens 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.

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.)

---

23 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.

24 Gemeint ist die bloße Betrachtung der Website, ohne dass etwa eine Registrierung erfolgt.

25 Vgl. Ansgar Koreng/Matthias Lachenmann: DatenschutzR-FormHdB, Form. F. I. 1. Anm. 6.

26 Vgl. Ansgar Koreng/Matthias Lachenmann: DatenschutzR-FormHdB, Form. F. I. 1. Anm. 8.

27 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 [26.08.2025].

Benennen von Speicherdauer bzw. Kriterien für die Festlegung derselben bezogen auf – Webserver-Log-Files – ggf., sofern eingesetzt, Cookies (**Hinweis:** Die zulässige Laufzeit von Cookies ist abhängig von deren Zweck. Soweit dies zur Zweckerreichung genügt, sind Cookies nach Ablauf der Sitzung („Session“) zu löschen. Dauerhafte, sog. persistente Cookies, bedürfen regelmäßig einer Einwilligung des Nutzers. Dies gilt insbes. für Werbe-Cookies.)	
Benennen des Bestehens der Betroffenenrechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit	
Benennen des Bestehens eines Beschwerderechts bei einer Aufsichtsbehörde	
Sofern zutreffend, zusätzliche Informationen erforderlich bzgl.:	**Check: ja/nein**
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: 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.	
Im Fall einwilligungsbasierter Datenverarbeitung: 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. (*Hinweis:* Da der Widerruf der Einwilligung so leicht sein soll wie deren Erteilung,[28] 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.)	

28 Art. 7 Abs. 3 S. 4 DSGVO.

In Fällen automatisierter Entscheidungsfindung einschließl. Profiling[29]:

- Umstand der automatisierten Entscheidungsfindung einschließl. Profiling
- aussagekräftige Informationen über die involvierte Logik sowie
- Tragweite und angestrebte 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**
Registrierungs- und Login-Prozess *Rechtsgrundlage Datenverarbeitung:* Ggf. Art. 6 Abs. 1 S. 1 lit. b DS-GVO, ansonsten regelmäßig Art. 6 Abs. 1 S. 1 lit. f DSGVO *Rechtsgrundlage Endgerätzugriffe:* § 25 Abs. 2 Nr. 2 TDDDG, sofern erforderlich für die Erbringung des konkreten Onlinedienstes	
Authentifizierungs-Cookies für die Dauer der Sitzung[30] *Rechtsgrundlage:* § 25 Abs. 2 Nr. 2 TDDDG (i. V. m. Art. 6 Abs. 1 lit. b oder f DSGVO)	
Verarbeitung von Informationen zu Online-Bestellungen, wie z. B. Versandadresse, Informationen zum bestellten Produkt, Zahlungsinformationen *Rechtsgrundlage:* Art. 6 Abs. 1 S. 1 lit. b DSGVO	
Warenkorbcookies[31] *Rechtsgrundlage:* § 25 Abs. 2 Nr. 2 TDDDG (i. V. m. Art. 6 Abs. 1 lit. b oder f DSGVO)	
Bonitätsprüfung, z. B. bei Online-Shops *Rechtsgrundlage:* Art. 6 Abs. 1 S. 1 lit. f DSGVO	
Datenverarbeitung im Zusammenhang mit einem Kontaktformular *Rechtsgrundlage:* Art. 6 Abs. 1 S. 1 lit. f DSGVO	

29 Art. 22 Abs. 1 und 4 DSGVO.
30 Die dauerhafte Speicherung beim Nutzer setzt dessen Einwilligung voraus.
31 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.

Einsatz von Tools zur Reichweitenmessung, d. h. zur statistischen Auswertung der Nutzung der Website (Tracking)

Rechtsgrundlage Datenverarbeitung: Art. 6 Abs. 1 S. 1 lit. f DSGVO oder Einwilligung

Rechtsgrundlage Endgerätzugriffe: § 25 Abs. 2 Nr. 2 TDDDG (str.)[32] bzw. Einwilligung

---

Interessengerechte Anzeige von Werbung basierend auf vorangegangenem Nutzerverhalten (Targeting)

Rechtsgrundlage Datenverarbeitung: ggf. Art. 6 Abs. 1 S. 1 lit. f DSGVO, ansonsten Einwilligung

Rechtsgrundlage Endgerätzugriffe: Einwilligung

Einbindung von Social Media Plug-ins von Facebook, X, Instagram u. Co.

Rechtsgrundlage: Einwilligung (mittels Zwei-Klick-Lösung bzw. Shariff[33])

Einbindung von Kartendiensten wie Google Maps

Rechtsgrundlage: Einwilligung (mittels Zwei-Klick-Lösung bzw. Shariff)

Einsatz von Webfonts wie z. B. Google Fonts

Prüfung im Einzelfall, notfalls Verzicht und nur lokale Einbindung von Fonts (alternativ: Einwilligung des Nutzers)

Zahlungsabwicklung, ggf. unter Einsatz von externen Dienstleistern

Rechtsgrundlage: Art. 6 Abs. 1 S. 1 lit. b oder f DSGVO

Newsletter Registrierung

Rechtsgrundlage: Einwilligung

Sonstige Zwecke (konkret benennen)

– Angabe der **Rechtsgrundlage** der Datenverarbeitung u./o. des Endgerätzugriffs
– Sofern zutreffend: 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**

---

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

33 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 [26.08.2025].

III. Sammlung weiterführender Links

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. (AWV)
Praxisleitfaden DSGVO-Umsetzung für KMU
DSGVO für kleine und mittlere Unternehmen (Stand 2022)
https://www.awv-net.de/dsgvo-kmu

Bundesministerium für Digitales und Verkehr (BMDV)
Bundesgesetz: Datenschutz bei digitalen Diensten und Telekommunikation
TDDDG (Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz)
https://www.gesetze-im-internet.de/ttdsg/TDDDG.pdf

Datenschutzkonferenz (DSK)
Aufsichtsbehörden: Vorgaben für digitale Dienste
Orientierungshilfe für Anbieter:innen von digitalen Diensten (Version 1.2, Nov. 2024)
https://www.datenschutzkonferenz-online.de/media/oh/OH_Digitale_Dienste.pdf

Europäische Union
EU-Datenschutz-Grundverordnung im Volltext
DSGVO (VO (EU) 2016/679)
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Europäische Union
EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation (Cookie-Richtlinie)
RL 2009/136/EG
https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32009L0136

IHK München
Checkliste und Hinweise für rechtssichere Websites
Rechtssichere Website
https://www.ihk-muenchen.de/ratgeber/recht/internetrecht/rechtssicherheit/

IHK Wiesbaden
Überblick rechtlicher Vorgaben beim Onlineauftritt
Internetauftritt: Rechtliche Anforderungen und Pflichten
https://www.ihk.de/wiesbaden/recht/rechtsberatung/internetrecht-und-werbung/internetauftritt-rechtliche-anforderungen-und-pflichten-1255572

LfD Niedersachsen (Landesbeauftragte für den Datenschutz)
Anforderungen an Consent-Banner aus Sicht der Aufsicht
Handreichung Datenschutzkonforme Einwilligungen auf Websites – Anforderungen an Consent-Layer (Sept. 2022)
https://lfd.niedersachsen.de/download/161158

Über den AWV-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 wird, sind z. B. die datenschutzrechtlichen Aspekte beim Cloud-Computing und beim Einsatz von 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 herangetragen 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 (Deutsche Industrie- und Handelskammer, Berlin).

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

aufgrund eines Beschlusses
des Deutschen Bundestages