Gesellschaft für Datenschutz
und Datensicherheit e.V.

# GDD-Praxishilfe DS-GVO

## ePrivacy und Datenschutz beim Onlineauftritt

INHALT

# 1. Einleitung

Betreiber von Websites, Apps und Co. haben die Vorgaben des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG), insbes. § 25 TDDDG, sowie die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) zu beachten. § 25 TDDDG setzt europäische Vorgaben, konkret: Art. 5 Abs. 3 ePrivacy-RL (RL 2002/58/EG), nahezu wortgleich in nationales Recht um. Die Interpretation der europäischen Norm kann insofern auch für die Auslegung und Anwendung der TDDDG-Bestimmung herangezogen werden. Ursprünglich war vorgesehen, dass zeitgleich mit der DS-GVO am 25.05.2018 auch eine diese ergänzende und die ePrivacy-RL ersetzende ePrivacy-VO als in allen EU-Mitgliedstaaten unmittelbar geltendes Recht in Kraft treten sollte. Dies ist nicht geschehen. Ob bzw. wann es noch zum Inkrafttreten der ePrivacy-VO kommen wird, ist unklar. Bis zur Geltung der ePrivacy-VO gilt das bestehende europäische ePrivacy-Recht fort, also die ePrivacy-RL in Fassung der sog. „Cookie Richtlinie" (Richtlinie 2009/136/EG).

Im Folgenden wird erläutert, auf welche Verhaltensweisen des Websitebetreibers § 25 TDDDG bzw. die DS-GVO konkret Anwendung finden, also ihr sachlicher Anwendungsbereich. Zudem wird der Rechtsrahmen dargestellt, der sich aus § 25 TDDDG bzw. der DS-GVO ergibt, also was konkret mit den personenbezogenen Daten der Websitenutzer/-innen gemacht werden bzw. unter welchen Voraussetzungen beim Einsatz von Cookies und Co. auf deren Endgeräte zugegriffen werden darf.

# 2. TDDDG

## 2.1 Anwendungsbereich des TDDDG

Das TDDDG enthält „besondere Vorschriften zum Schutz personenbezogener Daten bei der Nutzung von Telekommunikationsdiensten und digitalen Diensten", vgl. § 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.

Digitale Dienstleistungen ermöglichen die Nutzung digitaler Inhalte. Beispiele für digitale Dienste 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, Internetsuchmaschinen, Werbemails, aber auch bereits **„einfache" Homepages** zur Information über ein Unternehmen bzw. eine öffentliche Stelle.

## 2.2 Anforderungen an Cookies und Co. nach § 25 TDDDG

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

**Was sind Cookies?**[1]

Cookies sind kleine Textdateien, die der Webbrowser auf dem Computer speichert. Anhand von Cookies erkennt eine Website, wer sie gerade besucht, und kann dadurch Nutzerpräferenzen, wie z.B. Sprach- oder Log-in-Informationen speichern, damit der Nutzer die Einstellungen nicht immer wieder neu vornehmen bzw. sich immer wieder neu anmelden muss.

1 Die Erläuterungen zu den Cookies basieren auf den Ausführungen bei Schwartmann/Benedikt/Reif, Sonderveröffentlichung RDV 5/2020.

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 sog. persistente Cookies, die dauerhaft im System des Nutzers hinterlegt werden. Von diesen zu unterscheiden sind sog. 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.

Zum Schutz der Privatsphäre des Nutzers bei Nutzung von z.B. PCs, Laptops, Tablets oder Smartphones knüpft § 25 Abs. 1 TDDDG das Setzen und Auslesen von Cookies bzw. vergleichbare Verfahren im **Grundsatz** 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, wonach der Einsatz von Cookies & Co. keine Einwilligung des Nutzers erfordert, sofern Cookies unbedingt erforderlich sind zur Erbringung eines vom Nutzer ausdrücklich gewünschten Dienstes.

Als **einwilligungsfrei möglich** werden etwa nachfolgende Kategorien von Cookies angesehen, sofern die Cookies nicht für weitere Zwecke verwendet werden:[2]

>> **User-Input-Cookies (Session-ID)** 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. Beispiel: Warenkorbcookies

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

2 Art.-29-Datenschutzgruppe, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, WP 194 v. 07.06.2012, S. 7 ff., dort finden sich auch noch weitere Beispiele einwilligungsfrei möglicher Cookies.

>> **Nutzerorientierte Sicherheitscookies** (ob auch Cookies, die Sicherheitsinteressen der Anbieter/-in dienen, z.B. der Vermeidung von Klickbetrug, ist umstritten)

>> **Cookies zur Anpassung der Benutzeroberfläche**
Solche Cookies werden verwendet, um die nicht mit einer anderen dauerhaften Kennung wie etwa einem Benutzernamen verknüpften Einstellungen, z.B. Einstellung zur Sprache, für einen mehrere Webseiten umfassenden Dienst zu speichern.

Soweit auf einer Website nur einwilligungsfrei mögliche Cookies eingesetzt werden, bedarf es keines Cookie-Banners. Es genügt über die eingesetzten Cookies in der Datenschutzerklärung der Website zu informieren.

**Regelmäßig** als **einwilligungsbedürftig** anzusehen ist insbesondere das Setzen bzw. Auslesen von **Werbecookies** 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 digitalen Dienstes. 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 i.R.v. § 25 Abs. 2 Nr. 2 TDDDG aber nicht als ausreichend anzusehen.

Sind Endgerätzugriffe zur Reichweitenmessung/Webanalyse einwilligungsfrei möglich?

Viele Webseitenbetreiber 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 i.S.v. § 25 Abs. 2 Nr. 2 TDDDG sind, ist nicht abschließend geklärt. Nach Auffassung der französischen Datenschutzbehörde CNIL soll die Regelung eine „einfache" Webanalyse rechtfertigen können, vorausgesetzt, diese wird in anonymisierter Form vom Website-Betreiber selbst vorgenommen und dient ausschließlich der Fehlerbehebung, der Optimierung der technischen Performance oder auch der Analyse der konsultierten Inhalte.[3]

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.[4]

3 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 – 10.06.2021.

4 Vgl. hierzu LfDI BW FAQ „Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps", Version 2.0.1 (März 2022), S. 13 ff.

Anders als durch die DS-GVO werden durch § 25 TDDDG auch juristische Personen geschützt. Sofern mit dem Zugriff auf ein Endeinrichtung keine personenbezogenen Datenverarbeitungen einhergehen, ist allein das TDDDG maßgeblich. Gehen mit dem Endgerätezugriff auch personenbezogene Datenverarbeitungen einher, kommen insoweit § 25 TDDDG und die DS-GVO nebeneinander zur Anwendung.

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

## 2.3 Cookie-/Consent-Banner

Einwilligungen im Zusammenhang mit Cookies – und ggf. verbundenen Onlinedatenverarbeitungen[5] – werden üblicherweise mittels einer der Websitenutzung vorgeschalteten Abfrage eingeholt, die beim ersten Aufruf eingeblendet wird und in der Praxis als **sog. Cookie- oder auch Consent-Banner** bezeichnet wird. Banner, mit denen eine Einwilligung nach TDDDG und/oder DS-GVO eingeholt werden soll, müssen den **Anforderungen** genügen, **welche die DS-GVO an das Vorliegen einer wirksamen Einwilligung stellt** (Art. 7 DS-GVO, Art. 4 Nr. 11 DS-GVO). Für die TDDDG-Einwilligung ergibt sich dies über einen Verweis in § 25 Abs. 1 S. 2 TDDDG.

**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 aufgeführten Gesichtspunkte.**

**Unmissverständliche Erklärung oder sonstige eindeutige bestätigende Handlung**

- >> „Planet49"-Entscheidung[6] des EuGH: **Keine voreingestellten Ankreuzkästchen, aktive Handlung des Nutzers nötig**
- >> **Keine Einwilligung durch Weitersurfen** (str.)
- >> **Nudging**, d.h. Beeinflussung der Nutzerentscheidung durch optische Gestaltung der Schaltflächen, ist zulässig, solange es „maßvoll" erfolgt
- >> Nach DSK regelmäßig **„Reject All"-Button** auf erster Ebene des Cookie-Banners nötig (str.)

**Freiwilligkeit**

- >> Sog. **Kopplungsverbot** (Art. 7 Abs. 4 DS-GVO)

**Informiertheit**

- >> **Für wirksame Einwilligung nötige Mindestinformationen (allgemein):**[7]
  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 ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien nach Art. 46 DS-GVO

5 Vgl. dazu den Abschnitt zur DS-GVO.

6 EuGH, Urt. v. 01.10.2019 – C-673/17.

7 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 dazu, ob Dritte Zugriff auf die Cookies erhalten können.[8]

>> Beachtung der weitergehenden **Informationspflichten nach Art. 13 f. DS-GVO**

>> **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.

**Nachweis der Einwilligung:** Es genügt, nachzuweisen, dass/welche Prozesse implementiert wurden.

**Widerruf der Einwilligung**

>> Widerruf muss **so einfach wie die Erteilung** der Einwilligung sein (Art. 7 Abs. 3 S. 4 DS-GVO)

>> DSK: **„stets sichtbarer“ Direktlink bzw. Icon**

Nachfolgend finden sich **Gestaltungsvorschläge der französischen CNIL**. Abhängig von der Risikobereitschaft können auch andere Gestaltungen gewählt werden. Vertretbar erscheint z.B. eine leichte optische Betonung der Einwilligungs- im Verhältnis zur Ablehnoption (sog. Nudging). Konkrete **Gestaltungsvorschläge iS eines „Good Practice“** wurden auch iR einer Initiative von **ConPolicy** entwickelt (https://www.conpolicy.de/data/user_upload/Pdf_von_Publikationen/2023_01_26_Cookie_Guidelines.pdf).

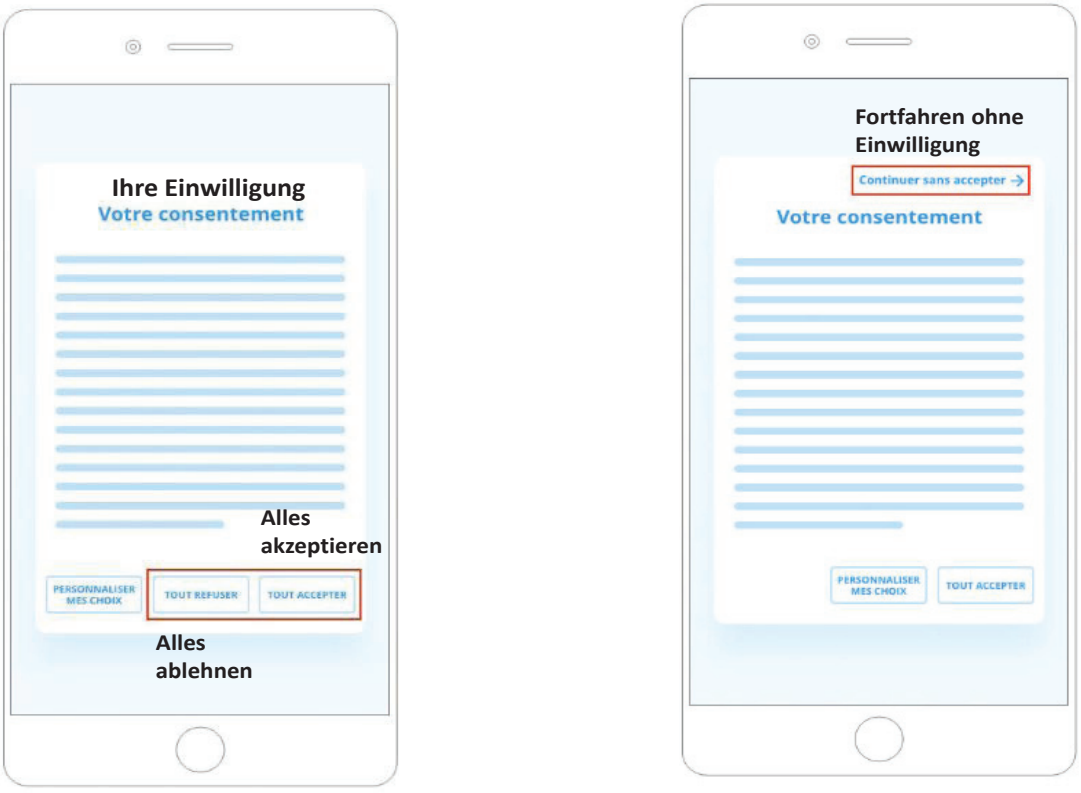


*Abbildung: Gestaltungsvorschläge für Cookie-Banner der französischen Datenschutzaufsicht CNIL*

8 EuGH, Urt. v. 01.10.2019 – C-673/17 („Planet49“-Entscheidung).

9 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»

**Wichtig: Websitebetreiber bleiben auch bei Einsatz sog. 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 nicht entlasten.**

## 2.4 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, konkret davon, ob hierzu ein „Zugriff" i.S.v. § 25 TDDDG auf das Endgerät stattfindet.

Beim sog. 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: ihre Browser – später wiedererkannt werden können. Zu den verwendeten Merkmalen zählen etwa Bildschirmauflösungen, Betriebssystemversionen, installierte Schriften oder Spracheinstellungen.

Die nationale Datenschutzkonferenz (DSK) lehnt eine umfassende Anwendung des § 25 TDDDG auf derartige Verfahren ab. Sie differenziert in ihrer Orientierungshilfe der Aufsichtsbehörden für Anbieter/-innen von Telemedien (nun digitale Dienste) zwischen dem Zugriff auf Daten, die beim Abruf eines Telemediendienstes (nun digitalen Dienstes) 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 TDDDG vor.[10]

# 3. DS-GVO

## 3.1 Anwendungsbereich der DS-GVO

Gemäß Art. 2 Abs. 1 ist die DS-GVO sachlich anwendbar, sofern **personenbezogene Daten ganz oder teilweise automatisiert verarbeitet** werden (Alt. 1) oder 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 DS-GVO regelt Ausnahmen von dem durch Abs. 1 vorgegebenen sachlichen Anwendungsbereich, wobei für den Bereich des Onlinedatenschutzes vor allem die sog. „**Haushaltsausnahme**" Bedeutung hat, nach welcher die DS-GVO keine Anwendung findet auf die Verarbeitung personenbezogener Daten durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten.

Bei den vorliegend relevanten Onlinesachver-

**10** DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter/-innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021), Version 1.1, Rn. 20 ff.

halten, also Verarbeitungen im Zusammenhang mit **Websites und Apps**, liegt stets auch eine ganz oder teilweise automatisierte Datenverarbeitung vor. Soweit Websites und Apps für **unternehmerische Zwecke** eingesetzt werden, kommt auch ein Eingreifen der Haushaltsausnahme nicht in Betracht.

Entscheidend für die Einschlägigkeit der DS-GVO auf Onlinesachverhalte ist damit regelmäßig v.a., inwiefern im Zusammenhang mit Websites und Apps personenbezogene Daten von Nutzer/-innen verarbeitet werden. Nach der Legaldefinition in Art. 4 Nr. 1 DS-GVO sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen [...]".

Informationen in diesem Sinne können etwa Name, Geschlecht, Kontoverbindung, Adresse oder Bestellinformationen i.R.d. 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 DS-GVO zu beachten ist?

Auf der Grundlage von Vorgaben des EuGH[11] hat der BGH[12] entschieden, dass die dynamische IP-Adresse für den Webseitenbetreiber ein personenbezogenes Datum darstellt. 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 Internetcafes oder offenen WLANS ohne Registrierungspflicht. Die theoretisch mögliche Unterscheidung zwischen personenbezogenen und nicht personenbezogenen 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.[13]

**11** EuGH, Urt. v. 19.10.2016 – C-582/14 (Rechtssache Breyer), Rn. 38 ff.
**12** BGH, Urt. v. 16.05.2017 – VI ZR 135/13.
**13** Kühling/Buchner/Klar/Kühling, DS-GVO Art. 4 Nr. 1 Rn. 36.

## 3.2 Anforderungen der DS-GVO an (Online-)Datenverarbeitungen und Verhältnis von DS-GVO und TDDDG

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 DS-GVO).

Als sonstige Rechtsgrundlagen im vorgenannten Sinne kommen insbesondere Art. 6 Abs. 1 lit. b und f DS-GVO in Betracht. Die erstgenannte Norm ermöglicht **erforderliche personenbezogene Datenverarbeitungen im Zusammenhang mit Verträgen** und bestimmten vorvertraglichen Konstellationen. 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 DS-GVO-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:[14]**

**Werden i.R. des Zugriffs auf die Endeinrichtung personenbezogene Daten verarbeitet, wird regelmäßig, wenn die Vorgaben von § 25 Abs. 2 TDDDG eingehalten sind, auch ein DS-GVO-Zulässigkeitstatbestand einschlägig sein, regelmäßig Art. 6 Abs. 1 Buchst. b (Vertrag) oder f (sog. Interessenabwägung). Bedarf es nach § 25 TDDDG der Einwilligung, so kann diese die personenbezogene Datenverarbeitung mit abdecken.**

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

So darf nach Erwägungsgrund 47 S. 7 DS-GVO 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 DS-GVO legitimiert werden.[15] Endgerätzugriffe zu Werbezwecken, insbes. Werbecookies, sind jedoch nach § 25 TDDDG einwilligungsbedürftig (vgl. oben unter 2.2). Der Endgeräteschutz nach TDDDG kennt anders als die DS-GVO keine Interessenabwägung.

## 3.3 Betroffenenrechte

### 3.3.1 Allgemeines

Betroffenenrechte sind Ansprüche und Gestaltungsmöglichkeiten, welche den von der personenbezogenen Datenverarbeitung betroffenen Personen zustehen. Diese können sich insbesondere, aber nicht nur aus der DS-GVO (Kapitel III und Kapitel VIII) ergeben. Innerhalb der Betroffenenrechte kommt dem Auskunftsrecht (Art. 15 DS-GVO) zent-

14 Schwartmann/Reif/Burkhardt im Heidelberger Kommentar zum TDDDG, § 25 Rn. 152 f.

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

rale Bedeutung zu, ist doch die Information darüber, ob und ggf. welche Daten der Verantwortliche über die betroffene Person verarbeitet, Grundvoraussetzung für die Geltendmachung weiterer Rechte, etwa auf Berichtigung, Löschung oder Schadensersatz. Auskunftsansprüche können auch gegenüber Webseitenbetreibern und sonstigen Onlineanbietern geltend gemacht werden. Hierauf soll im Folgenden ebenso näher eingegangen werden wie auf das Recht auf bzw. die Pflicht zur Datenlöschung (Art. 17 DS-GVO) im Zusammenhang mit Onlineangeboten.

### 3.3.2 Auskunft

Nach Art. 15 Abs. 1 DS-GVO hat die betroffene Person das Recht, vom Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Sofern dies der Fall ist, hat sie Anspruch auf Erteilung weiterer, gesetzlich definierter Einzelinformationen zur Datenverarbeitung und den insoweit bestehenden Datenschutzrechten.

Wird der **Auskunftsanspruch gegenüber einem Webseitenbetreiber** geltend gemacht, so richtet sich dieser u.a. auf die mit dem Nutzer ausgetauschten Kommunikationsinhalte, also z.B. bei einem Onlineshop Informationen zu den bestellten Produkten und zur Bezahlung und Lieferung der gekauften Ware. Der Auskunftsanspruch bezieht sich also auf die im Onlineshop-System vorhandenen (Inhalts-)Daten. Dem Auskunftsanspruch unterliegen aber auch vom Verantwortlichen zum jeweiligen Nutzer gespeicherte Zugangsinformationen sowie, soweit vorhanden, Informationen zum jeweiligen Nutzerverhalten (Seitenbesuche, aufgerufene Informationen, Downloads etc.).

Da auch für IP-Adressen regelmäßig von einer Personenbeziehbarkeit auszugehen ist,[16] ist eine praxisrelevante Frage, inwiefern sich ein geltend gemachter Auskunftsanspruch auch auf vom Verantwortlichen **mitgeloggte IP-Adressen** bezieht. Insofern ist zu differenzieren. Wird die IP-Adresse in einem Zusammenhang mitgeloggt, in dem der zugehörige surfende Nutzende für den Webseitenbetreiber nicht zu identifizieren ist, kann sich der/die Verantwortliche auf Art. 11 Abs. 1, Abs. 2 S. 2 DS-GVO berufen.[17] Sofern IP-Adressen allein aus Gründen der Datensicherheit gespeichert werden, um die Stabilität und die Betriebssicherheit des Internetauftritts zu gewährleisten,[18] und separat verarbeitet werden, kann eine Ausnahme von der Auskunftspflicht im Übrigen ggf. über § 34 Abs. 1 Nr. 2 b) BDSG begründet werden. Wird die IP-Adresse hingegen z.B. im Rahmen eines Bestellvorgangs durch einen angemeldeten Nutzer gespeichert, greift keine Ausnahme von der Auskunftspflicht.

### 3.3.3 Löschung

Gemäß Art. 17 DS-GVO kann die betroffene Person vom Verantwortlichen die unverzügliche Löschung ihn betreffender personenbezogener Daten verlangen und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der in Abs. 1 der Vorschrift genannten Löschgründe vorliegt und im konkreten Fall kein Ausnahmetatbestand nach Abs. 3 eingreift. Ein Löschgrund besteht insbes., wenn personenbezogene **Daten** für die Zwecke, zu denen sie erhoben oder sonst verarbeitet wurden, **nicht mehr notwendig sind** (Zweckfortfall, Art. 17 Abs. 1 lit. a DS-GVO). Ausnahmen von der Löschpflicht können sich insbes. ergeben, sofern einer Datenlöschung handels- oder steuerrechtliche **Aufbewahrungspflichten** entgegenstehen (Art. 17 Abs. 3 lit. b DS-GVO).

**16** Vgl. hierzu oben unter 3.1.

**17** Franck in: Gola/Heckmann, DS-GVO BDSG, Art. 12 Rn. 32.

**18** In diesem Fall sind für die Logfiles angemessene Löschfristen festzulegen, vgl. dazu auch den nachfolgenden Abschnitt zur Datenlöschung.

**Da die Löschverpflichtung des Verantwortlichen unabhängig von einem Antrag der betroffenen Person besteht, sollte jede/r Verantwortliche, der/die personenbezogene Daten verarbeitet, über ein Konzept zur Datenlöschung verfügen. Die Löschfristen sind dabei für jede verarbeitete Datenart individuell zu bestimmen.**

**Webserver-Logfiles dürfen zu eigenen Sicherheitszwecken gespeichert werden, um die Stabilität und die Betriebssicherheit des Internetauftritts zu gewährleisten, sind aber zeitnah wieder zu löschen, soweit kein Zwischenfall aufgetreten ist.**

**Hinsichtlich der konkreten Löschfrist orientiert sich die Praxis vielfach an einer BGH-Entscheidung aus 2014, wonach Internetserviceprovider IP-Adressen der Nutzer für maximal sieben Tage anlasslos speichern dürfen, um Netzstörungen und Fehler zu verhindern.[19] Nach dem Bayerischen Landesamt für Datenschutzaufsicht soll auch eine Löschfrist von 30 Tagen genügen.[20]**

Soweit **Kundendaten im Zusammenhang mit einem Onlineshop** verarbeitet werden, sind die handels- und steuerrechtlichen Aufbewahrungsfristen zu beachten, wonach etwa Rechnungen und Buchungsbelege für einen Zeitraum von 10 Jahren vorzuhalten sind. Solange entsprechende Fristen laufen, dürfen personenbezogene Daten auch dann nicht gelöscht werden, wenn die betroffene Person es verlangt.

Verlangt ein Kunde vom Onlineshop-Betreiber die **Löschung seines Kundenkontos**, ist dieser verpflichtet dem Löschwunsch des Kunden zu entsprechen. Daten, die aus gesetzlichen Gründen gespeichert bleiben müssen, sind für den laufenden Betrieb zu sperren und separat aufzubewahren.[21] Angesichts des Grundsatzes der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DS-GVO) sind Verantwortliche im Übrigen verpflichtet Löschkonzepte zu erstellen, in denen festgelegt ist, wann inaktive („verwaiste“) Kundenkonten gelöscht werden.[22]

## 3.4 Datenschutzerklärung

Ein zentraler Grundsatz der DS-GVO ist das Erfordernis der **Transparenz der personenbezogenen Datenverarbeitung** (Art. 5 Abs. 1 lit. a DS-GVO). Die von der Verarbeitung betroffene Person, hier der/die Internetnutzer/-in, soll nachvollziehen können, wer ihre/seine Daten zu welchen Zwecken verarbeitet. Hinsichtlich der Datenverarbeitungen im Zusammenhang mit einer Webseite dies dadurch gewährleistet, dass der Anbieter auf seiner Seite Informationen zum Datenschutz zur Verfügung zu stellen hat (sog. „**Datenschutzerklärung**“). Die konkrete Verpflichtung, solche Informationen vorzuhalten, ergibt sich aus Art. 13 DS-GVO, der die Informationspflichten bei Erhebung personenbezogener Daten bei der betroffenen Person regelt. Die Datenschutzerklärung sollte von jeder Unterseite der Website aus **mit einem Klick erreichbar** sein.[23]

19 BGH, Urteil vom 3. Juli 2014 – III ZR 391/13.
20 https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf.

21 BayLDA, 28. Tätigkeitsbericht 2018, S. 146.
22 LfDI Berlin, Jahresbericht 2018, S. 125 und 132.
23 Art.-29-Datenschutzgruppe WP 260 rev.01 Rn. 11; bei Apps ist eine ausreichende Erreichbarkeit nach dem Papier auch dann gegeben, wenn zum Aufruf der Erklärung zwei Klicks getätigt werden müssen. Beim Impressum, vgl. dazu unter 4., sollen generell zwei Klicks ausreichend sein, BGH Urt. v. 20.03.2006 – I ZR 228/03.

Den Vorgaben an die Erreichbarkeit wird vielfach durch Aufnahme eines Links im Header oder Footer neben dem Impressum nachgekommen.

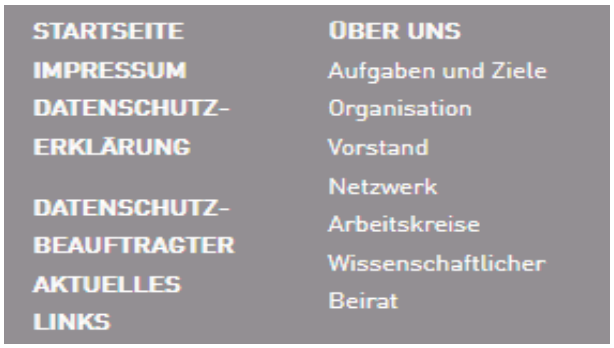


*Abbildung: Footer der GDD-Website mit Link zu Impressum und Datenschutzerklärung (Beispiel)*

Ein allgemein gültiges Muster für die Datenschutzerklärung 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.

Notwendige Mindestinformationen im Rahmen der **Datenschutzerklärung** sind:

- Name und Kontaktdaten des Verantwortlichen, z.B. des die Webseite betreibenden Unternehmen
- Kontaktdaten des Datenschutzbeauftragten (DSB) (soweit benannt) (Hinweis: Die Angabe des Namens ist nicht notwendig.)
- Zwecke, für die personenbezogene Daten verarbeitet werden, sowie die jeweilige Rechtsgrundlage
- Sofern die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DS-GVO (Interessenabwägung) erfolgt: Angabe der verfolgten berechtigten Interessen
- Datenempfänger bzw. Kategorien von Datenempfängern (soweit relevant)
- Beabsichtigter Drittlandtransfer von Daten (soweit relevant)
- Dauer der Datenspeicherung bzw. Kriterien für die Festlegung der Dauer, z.B. im Hinblick auf die Webserver-Log-Files
- Informationen zu den Datenschutzrechten der Nutzer/-innen

Typischerweise werden folgende **Themen** in der Datenschutzerklärung einer Website behandelt:

- Bereitstellung der Website und Verarbeitung von Log-Files
- Registrierungs- und Log-in-Prozess
- Verarbeitung von Informationen aus Online-Bestellungen
- Bonitätsprüfung, z.B. bei Online-Shops
- Datenverarbeitung im Zusammenhang mit einem Kontaktformular
- Einsatz von Tools zur Reichweitenmessung, d.h. zur statistischen Auswertung der Nutzung der Website (Tracking)
- Interessengerechte Anzeige von Werbung basierend auf vorangegangenem Nutzerverhalten (Targeting)
- Einbindung von Social Plug-ins von Facebook, Twitter, Instagram und Co.
- Einbindung von Kartendiensten, wie Google Maps
- Einsatz von Webfonts, wie z.B. Google Fonts
- Zahlungsabwicklung, ggf. unter Einsatz von externen Dienstleistern

**Die Datenschutzerklärung ist ein reiner Informationstext. Sie ist kein tauglicher Ort, um Einwilligungserklärungen der Nutzenden in Datenverarbeitungen im Zusammenhang mit der Webseite einzuholen, und sollte von etwaigen Allgemeinen Geschäftsbedingungen (AGB) getrennt werden.**[23]

**23** Schwartmann/Benedikt/Reif, Datenschutz und ePrivacy, 2020, S. 65 f.

## 4. Anbieterkennzeichnung („Impressum“)

Praktisch jede Webseite benötigt eine sog. Anbieterkennzeichnung. In der Praxis hat sich für die Anbieterkennzeichnung auch der Begriff „Impressum“ durchgesetzt. Der Umstand, dass man eine Anbieterkennzeichnung braucht, ergibt sich aus § 5 Digitale-Dienste-Gesetz (DDG), der auch die notwendigen Inhalte regelt. Es handelt sich hierbei nicht um eine datenschutzrechtliche Pflicht, sondern eine allgemeine Vorgabe an die Anbieter/in von digitalen Diensten. Die Pflicht, eine Anbieterkennzeichnung zu haben, besteht z.B. auch für private Websites, Blogs oder Fanpages bei Facebook.

Nutzer/-innen sind mit Hilfe der Anbieterkennzeichnung in der Lage, Diensteanbieter auf ihre Seriosität zu überprüfen, bevor sie deren Dienste in Anspruch nehmen. Aber auch Unternehmen haben ein erhebliches Interesse daran, die erforderlichen Informationen über andere Marktteilnehmer zu erlangen, um ein wettbewerbsrechtlich einwandfreies Verhalten durchsetzen zu können. Die Informationen, die im Rahmen der Anbieterkennzeichnung zur Verfügung zu stellen sind, entsprechen im Wesentlichen denjenigen, die Handelsunternehmen im traditionellen Rechts- und Geschäftsverkehr beispielsweise auf Geschäftsbriefen ohnehin bereitstellen müssen.

Nähere Informationen zu den notwendigen Inhalten der Anbieterkennzeichnung finden sich z.B. in den diesbezüglichen Onlinepublikationen der IHKs.

Die Anbieterkennzeichnung muss nach dem DDG „leicht erkennbar, unmittelbar erreichbar und ständig verfügbar“ sein. Unmittelbare Erreichbarkeit wird dabei in der Praxis angenommen, sofern die Anbieterkennzeichnung über **max. zwei Klicks** erreichbar ist.[25] Für die Anbieterkennzeichnung und die Datenschutzerklärung sollten jeweils eigene Bereiche innerhalb des Webauftritts vorgesehen werden.

**25** BGH Urt. v. 20.03.2006 – I ZR 228/03.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

# Mitglied werden? Mehr Informationen?

**https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de**

**Eine Mitgliedschaft bietet wesentliche Vorteile:**

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „DataAgenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

**Herausgeber:**
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 228 96 96 75-00
Fax: +49 228 96 96 75-25
www.gdd.de
info@gdd.de
Ansprechpartnerin: RAin Yvette Reif, LL.M.
Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

**Stand:**
Version 1.2 (Mai 2024)