



## FAQ

# Cookies und Tracking durch Betreiber von Webseiten und Hersteller von Smartphone-Apps



Der Landesbeauftragte für  
Datenschutz und  
Informationsfreiheit  
Baden-Württemberg

Herausgegeben vom  
Landesbeauftragten für den Datenschutz und die Informationsfreiheit  
Dr. Stefan Brink  
Lautenschlagerstraße 20, 70173 Stuttgart  
Telefon: 0711/615541-0  
Telefax: 0711/615541-15  
<https://www.baden-wuerttemberg.datenschutz.de>  
E-Mail: [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de)  
Mastodon: <https://bawue.social/@lfdi>  
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962  
Umschlagbild: bakhtiarzein - stock.adobe.com  
Version 2.0.1, Stand März 2022

# Inhalt

<b>Inhalt</b> .....	<b>3</b>
<b>Vorbemerkung</b> .....	<b>5</b>
<b>Abschnitt A: Fragen und Antworten</b> .....	<b>7</b>
1. Cookies und vergleichbare Techniken .....	7
1.1. Braucht jede Webseite einen Cookie- oder Einwilligungs-Banner? .....	7
1.2. Was bedeutet „Speichern oder Auslesen von Informationen auf dem Endgerät“? .....	7
1.3. Welche Cookies und andere Techniken darf ich ohne Einwilligung nutzen? .....	7
1.4. Für welche Cookies und Tracking-Mechanismen brauche ich die Einwilligung der Nutzenden?.....	8
1.5. Sollten Webseiten sicherheitshalber Einwilligungen per (Cookie-)Banner einholen, auch wenn dies nicht nötig ist? .....	9
2. Einbindung externer Inhalte/(Medien-)Elemente.....	9
2.1. Wie kann ich Social-Media-Buttons einbinden?.....	11
2.2. Wie kann ich externe Inhalte von Twitter, YouTube, Facebook und Co. einbinden? .....	11
2.3. Wie kann ich (externe) Kartendienste einbinden? .....	12
2.4. Wie kann ich (externe) Schriftarten/Fonts einbinden?.....	12
2.5. Was muss bei Anbietern beachtet werden, die Daten außerhalb der EU übermitteln (Drittstaatentransfer)? .....	13
3. Reichweitenanalyse .....	13
3.1. Darf ich Werkzeuge zur Reichweitenanalyse ohne Einwilligung der Nutzenden verwenden? .	14
3.2. Was ist serverseitiges Tracking und kann ich damit Vorgaben des TTDSG oder der DS-GVO umgehen? .....	16
4. Anforderungen an Einwilligungs-Banner .....	18
4.1. Auf welchen Unterseiten sind Einwilligungs-Banner erforderlich? .....	18
4.2. Was sind die Anforderungen an die informierte, freiwillige, aktive und vorherige Einwilligung? .....	18
4.3. Wie gestalte ich Einwilligungs-Banner? .....	20
4.4. Welche Informationen müssen in Einwilligungs-Bannern zum Zweck gegeben werden? .....	21
4.5. Können Standards der Werbeindustrie zum Einholen von Einwilligungen bedenkenlos verwendet werden? .....	22
4.6. Was muss bei Gesundheitsdaten, Daten zur sexuellen Orientierung, politischen Meinungen und anderen besonderen Kategorien personenbezogener Daten beachtet werden? .....	22
4.7. Können jegliche Verarbeitungen durchgeführt werden, wenn eine wirksame Einwilligung eingeholt wurde?.....	22
<b>Abschnitt B: Negativbeispiele und „Standardfehler“</b> .....	<b>23</b>
1. Einhaltung der Bedingungen für wirksame Einwilligungen .....	23
1.1. Vorherige Einwilligung.....	23
1.2. Freiwillige Einwilligung .....	23
1.3. Informiertheit.....	24

## FAQ zu Cookies und Tracking

1.4. Aktive Einwilligung.....	26
1.5. Separat von anderen Erklärungen.....	27
1.6. Widerruflichkeit.....	27
2. Rechtmäßigkeit, Fairness und Transparenz.....	27
2.1. Rechtmäßigkeit.....	27
2.2. Verarbeitung nach Treu und Glauben.....	27
2.3. Transparenz.....	28
3. Datenverarbeitung ohne Einwilligung.....	29
3.1. Vertrag.....	29
3.2. Berechtigtes Interesse .....	29
4. Einhaltung der Betroffenenrechte.....	30
5. Drittstaatentransfer.....	31
6. Auftragsverarbeitung.....	31
7. Gemeinsame Verantwortung.....	32
<b>Abschnitt C: Beispiele für Banner .....</b>	<b>33</b>

## Vorbemerkung

Betreiber von **Webseiten** oder Hersteller von **Apps** für mobile Endgeräte (z.B. Smartphone, Tablet) müssen als Verantwortliche<sup>1</sup> sicherstellen, dass bei der Verarbeitung personenbezogener Daten alle Vorgaben der Datenschutz-Grundverordnung (DS-GVO) eingehalten werden. Sie sind zugleich Anbieter von Telemediendiensten nach dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG, hier: § 2 Abs. 2 Nr. 1), welches die Nutzung von Cookies und ähnlichen Technologien zum Ablegen oder Auslesen von Informationen auf den Systemen regelt; solche Technologien werden häufig zur Wiedererkennung von Nutzenden verwendet und sind inzwischen extrem weit verbreitet.

Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden der Länder und des Bundes (Datenschutzkonferenz, DSK) hat im Dezember 2021 mit der „Orientierungshilfe der Aufsichtsbehörden für die Anbieter:innen von Telemedien (OH Telemedien 2021)“<sup>2</sup> rechtliche und technische Erläuterungen zur Anwendung der DS-GVO und des TTDSG gegeben. Diese FAQ soll diese Ausführungen unter Einbeziehung konkreter Anwendungsfälle praxisorientiert ergänzen.

Die FAQ bezieht sich im Wesentlichen auf Webseiten, gilt sinngemäß aber auch für **sonstige Telemedien** wie Smartphone- und Tablet-Apps, PC-Software oder Geräte aus dem Bereich des Internets der Dinge (Internet of Things, IoT) wie vernetzte Küchengeräte, Lampen, Steuergeräte für Heizungen, Alarmsysteme, Smart-TVs oder vernetzte Fahrzeuge, wenn und soweit diese über entsprechende Kommunikationsfunktionen verfügen.

Die folgende FAQ beantwortet zuerst (Abschnitt A) häufige Fragen in Bezug auf **Cookies und Tracking** und gibt sodann einen Überblick zu möglichen **datenschutzfreundlicheren Lösungen** bei der **Einbindung von (Medien-) Inhalten** und zur sog. **Reichweitenanalyse**. Weiterhin enthält dieses Dokument Hinweise dazu, welche Bedingungen eingehalten werden müssen, wenn Verantwortliche – also die Betreiber von Websites, Apps oder anderen Telemediendiensten – sich dazu entscheiden, Verarbeitungen oder Techniken zu nutzen, die **Einwilligungen** erfordern. Anschließend wird in den Abschnitten B und C anhand von typischen, in der Prüfpraxis häufig auftretenden **Standardfehlern** dargestellt, wie eine Umsetzung in der Praxis nicht erfolgen darf.

Weitere Informationen sind der Orientierungshilfe (OH Telemedien 2021) zu entnehmen.

### Unterschiede DS-GVO zu TTDSG (bzw. ePrivacy-Verordnung)

Während die DS-GVO dem Schutz personenbezogener Daten dient, regelt das TTDSG in § 25 den Einsatz von Cookies und ähnlichen Technologien, mittels derer Informationen auf Endeinrichtungen<sup>3</sup> gespeichert oder aus diesen ausgelesen werden – und zwar unabhängig davon, ob diese personenbezogen sind oder nicht. Das TTDSG schützt also vor allem die Integrität von Endeinrichtungen bzw.

---

<sup>1</sup> Zur Definition des Begriffs „Verantwortliche“ siehe auch Artikel 4 Nr. 7 DS-GVO.

<sup>2</sup> Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien, siehe [https://www.datenschutzkonferenz-online.de/media/oh/20211220\\_oh\\_telemedien.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20211220_oh_telemedien.pdf)

<sup>3</sup> Zur Definition des Begriffs „Endeinrichtung“ siehe § 2 Absatz 2 Nr. 6 TTDSG

schützt sie vor Fremdzugriff. Vergleichbar ist das TTDSG insoweit mit der Unverletzlichkeit der Wohnung (Artikel 13 GG), die vor unbefugtem Zutritt schützt.

Die sich an den Zugriff anschließende Verarbeitung personenbezogener Daten, z. B. zur Bildung von Nutzer\_innenprofilen, wird vom TTDSG dagegen nicht erfasst. Diese Verarbeitung unterliegt vollständig der DS-GVO, die den Umgang mit personenbezogenen Daten<sup>4</sup> regelt.

TTDSG und DS-GVO gelten somit nebeneinander.

Diese FAQ ersetzt die FAQ zu Cookies und Tracking in Version 1.0.1 vom 29. April 2019 unter <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/FAQ-zu-Cookies-und-Tracking.pdf> vollständig.

---

<sup>4</sup> Zur Definition des Begriffs „personenbezogene Daten“ siehe Artikel 4 Nr. 1 DS-GVO.

## Abschnitt A: Fragen und Antworten

### 1. Cookies und vergleichbare Techniken

#### 1.1. Braucht jede Webseite einen Cookie- oder Einwilligungs-Banner?

**Nein.** Soweit keine einwilligungsbedürftigen Verarbeitungen vorgenommen werden, ist nach DSGVO auch keine Einwilligung nötig. Nach TTDSG ist keine Einwilligung nötig, wenn keine Informationen auf den Endgeräten der Nutzenden abgelegt oder von dort ausgelesen werden, die nicht unbedingt erforderlich sind, damit von den Nutzenden ausdrücklich gewünschte Dienste zur Verfügung gestellt werden können.

Es empfiehlt sich daher schon zur Begrenzung des eigenen Aufwands, so weit möglich auf Cookies und einwilligungsbedürftige Verarbeitungen zu verzichten. Damit vermeiden Betreiber von Internetangeboten und anderen Telemediendiensten auch die umfangreichen Herausforderungen bei der korrekten Einholung von Einwilligungen.

#### 1.2. Was bedeutet „Speichern oder Auslesen von Informationen auf dem Endgerät“?

§ 25 TTDSG bezieht sich auf „die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder den Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind“. Gemeint ist damit beispielsweise der Einsatz von Cookies und anderen Technologien wie LocalStorage, Web Storage, das Auslesen von Werbe- und Geräte-IDs, Seriennummern, aber auch der Einsatz von ETags oder TLS-Session-IDs zum Zwecke des Trackings, Fingerprinting (z.B. durch das Auslesen von installierten Schriften oder Anwendungen) und vieles mehr. Der Einfachheit halber wird das im Folgenden i.d.R. unter dem verkürzenden Begriff „Cookies“ zusammengefasst.

Weitere Informationen dazu finden sich in der OH Telemedien, Seite 7 ff.

#### 1.3. Welche Cookies und andere Techniken darf ich ohne Einwilligung nutzen?

Cookies sind grundsätzlich einwilligungsbedürftig (siehe § 25 Absatz 1 Satz 1 TTDSG). Dies betrifft wie zuvor dargelegt auch andere Technologien, die Informationen auf dem Endgerät der Nutzer\_innen ablegen oder von ihnen auslesen.

Von der Einwilligungspflicht nach dem TTDSG ausgenommen sind Cookies, die (insbesondere technisch) unbedingt erforderlich (auch als „notwendig“ bzw. „essentiell“ bezeichnet) sind, um den von Nutzer\_innen nachgefragten Dienst zu erbringen. Dazu zählen z. B.:

- Notwendige Sitzungsverwaltung (z.B. Login oder Warenkorb-Cookies, sobald ein\_e Nutzer\_in sich anmeldet bzw. ein Produkt in den virtuellen Einkaufswagen legt)
- Nutzer\_inneneingaben, die sich bei Onlineformularen über mehrere Seiten erstrecken, sobald Nutzer\_innen das Formular ausfüllen
- Ausgewählte Sprache, sofern die Standardeinstellung verändert wird

- Vermerken des Einwilligungsstatus, aber nur mittels Angabe des Status (ja/nein), nicht einer eindeutigen ID
- Einsatz zu Sicherheitszwecken in sehr engen Ausnahmefällen und grundsätzlich nur bei gesonderter Nutzer\_innen-Interaktion (z.B. bei Abstimmung mittels eines Abstimmungs-Tools, um Mehrfachabstimmungen zu erschweren)

Diese **Notwendigkeit ergibt sich aber nicht** daraus, dass eine bestimmte Software mit Cookies implementiert wurde, sondern danach, ob die Nutzung von Cookies für den angestrebten Zweck **unbedingt erforderlich** ist, damit der Anbieter einen von den Nutzenden ausdrücklich gewünschten Dienst zur Verfügung stellen kann. Beispielsweise ist es grundsätzlich nicht notwendig, beim bloßen Aufrufen einer Webseite einen Cookie mit einer Session-ID zu setzen. Auch **die zeitliche Dimension** ist zu betrachten: Cookies oder andere Techniken dürfen erst ab dem Zeitpunkt einwilligungsfrei genutzt werden, ab dem sie unbedingt **erforderlich** sind und nicht bereits vorher.

Neben den Vorgaben des TTDSG benötigt die Verarbeitung personenbezogener Daten eine Rechtsgrundlage nach der DS-GVO. Diese kann beispielsweise ebenfalls eine Einwilligung sein. Bei der Verarbeitung personenbezogener Daten können sich Verantwortliche häufig bei (vor-)vertraglichen Maßnahmen auf Artikel 6 Absatz 1 Buchstabe b DS-GVO stützen. Dies ist z.B. bei der Verwendung einer Warenkorb-Funktion der Fall, wenn dabei keine Übertragung von Daten an Dritte bzw. keine Einbindung von Elementen Dritter stattfindet.

Weitere Informationen zu dieser Thematik und über Ausnahmen von der Einwilligungsbedürftigkeit finden sich in der Orientierungshilfe (OH Telemedien 2021) ab Seite 18 ff.

#### **1.4. Für welche Cookies und Tracking-Mechanismen brauche ich die Einwilligung der Nutzenden?**

Gemäß § 25 Absatz 1 Satz 1 TTDSG bedarf die Speicherung von Informationen wie Cookies in der Endeinrichtung oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, grundsätzlich der Einwilligung der Nutzenden. Von dem Grundsatz der Einwilligungsbedürftigkeit sind in § 25 Absatz 2 TTDSG Ausnahmen vorgesehen. Diese finden im Zusammenhang mit Cookies bzw. Techniken wie Web-Bugs oder Browser-Fingerprinting, die das Tracking des Nutzenden zum Ziel haben, jedoch keine Anwendung. Sie sind technisch „nicht erforderlich“, um den Telemediendienst bereitzustellen.

Anbieter von Telemediendiensten, die Elemente integrieren, welche das Nutzer\_innenverhalten insbesondere über Website- oder Geräte-Grenzen hinweg (also z.B. über verschiedene Domains verschiedener Anbieter) zusammenfassen, benötigen auch nach der DS-GVO die aktive, ausdrückliche, informierte, freiwillige und vorherige Einwilligung (Artikel 6 Absatz 1 Buchstabe a DS-GVO) der Nutzenden (vgl. Seite 9 ff. der OH Telemedien 2021 und den folgenden Abschnitt A 4 dieser FAQ). Dies gilt insbesondere (aber nicht nur) für die Einbindung von Plugins von Social-Media-Anbietern, großen Online-Plattform-Betreibern und Werbenetzwerken.

Aber auch der Betreiber selbst darf nicht beliebig personenbezogene Daten der Nutzer\_innen ohne Einwilligung zusammenführen oder anderweitig verarbeiten, auch insoweit gilt die DS-GVO.

### 1.5. Sollten Webseiten sicherheitshalber Einwilligungen per (Cookie-)Banner einholen, auch wenn dies nicht nötig ist?

**Nein!** Unbedingt erforderliche Cookies benötigen keine Einwilligung nach TTDSG und eine Einwilligung nach DS-GVO wäre die falsche Rechtsgrundlage. Denn diese eingeholte Einwilligung suggeriert, dass die Verarbeitung freiwillig ist und Nutzende diese jederzeit mit Wirkung für die Zukunft widerrufen könnten, obwohl das rechtlich nicht möglich ist. Ein Banner schadet in einem solchen Fall also:

Betroffenen zu suggerieren, sie könnten ihre Einwilligung widerrufen, obwohl dies gar nicht der Fall ist (also eine andere Rechtsgrundlage als die Einwilligung herangezogen wird), verstößt gegen die Grundsätze von Treu und Glauben sowie der Transparenz, da es sich um eine falsche und irreführende Information handelt (vgl. Artikel 5 Absatz 1 DS-GVO sowie Artikel 12 Absatz 1 in Verbindung mit Artikel 13 Absatz 2 Buchstabe c DS-GVO).

## 2. Einbindung externer Inhalte/(Medien-)Elemente

Webseiten können aus verschiedenen Elementen (z.B. Textteile, Bilder, Schriften) zusammengesetzt sein. Diese Elemente können sowohl in der HTML-Datei des Dokuments des Anbieters vorliegen als auch aus separaten Dateien geladen werden. Daneben kann Programmcode als Element (z.B. JavaScript oder WebAssembly) ausgeführt werden.

Abrufe können von Servern des Anbieters der Webseite erfolgen, aber auch von Drittanbietern<sup>5</sup>.

Verbindungen zu externen Servern können technisch in verschiedener Weise durchgeführt werden:

- Betreiber von Telemediendiensten können durch Anweisungen im HTML-Quellcode der Webseite oder durch JavaScript-Befehle den Webbrowser der Nutzer\_innen dazu veranlassen, sich mit Servern von Drittanbietern zu verbinden und dabei personenbezogene Daten zu übertragen bzw. Inhalte von dort abzurufen.
- Daneben kann im Kontext des Besuchs der Webseite serverseitig eine Übertragung von (personenbezogenen) Daten an einen Server eines Drittanbieters erfolgen bzw. können von dort Inhalte abgerufen werden.

Der Bedarf der Einbindung externer Inhalte/(Medien-)Elemente kann sich aus verschiedenen Gründen ergeben.

Drittanbieter bieten etwa die Möglichkeit, Kartendienste einzubinden oder Beiträge aus sozialen Medien wie Twitter oder Facebook, Links auf Social-Media-Präsenzen, Videos, Zahlungsdienstleister, Webseiten-Analysedienste oder Schriftarten auf einfache Weise zu integrieren.

---

<sup>5</sup> Im Rahmen dieses Dokuments wird zur Vereinfachung der Darstellung einheitlich der Begriff „Drittanbieter“ verwendet und hinsichtlich der Verantwortlichkeit nicht nach DS-GVO differenziert. Unter diesen Begriff fallen dabei auch Auftragsverarbeiter nach Artikel 4 Nr. 8 DS-GVO. Ebenfalls erfolgt keine Differenzierung zwischen „Produkten“, „Diensten“ (z.B. Programmlogik mit API-Zugang) oder reinen Inhalten (Assets).

Durch die Einbindung (z.B. durch HTML oder JavaScript) der externen Elemente der Drittanbieter durch den Anbieter des Telemediendienstes wird der Browser des Nutzens dazu angeleitet, eine Verbindung mit dem Server des Dritten aufzubauen. Dadurch kommt es zu Datenübermittlungen an den Drittanbieter (mindestens der IP-Adresse des Nutzens, aber auch der Webseite, von der aus der Zugriff erfolgt als sog. URL-Referrer) bzw. ggf. der Speicherung/dem Auslesen von Informationen aus dem Endgerät der Nutzens. Der Anbieter kann unter Umständen (z.B. bei erfolgtem Login des Nutzens beim Drittanbieter) diese Informationen mit bereits bei sich gespeicherten Informationen über den Nutzens verketten, erhält also u.U. sehr detaillierte Informationen über die Interessen der betroffenen Person außerhalb der eigenen Plattform.

Im Ergebnis gestattet der Anbieter des Telemediendienstes durch die Einbindung somit dem Drittanbieter, (personenbezogene) Daten der Nutzer\_innen zu verarbeiten bzw. Informationen auf den Endgeräten zu speichern, auszulesen sowie diese mit weiteren Daten aus anderen Quellen zu verknüpfen. Vergleichbar wäre, wenn ein lokaler Einzelhändler dem Anbieter von Plakatwerbung gestatten würde, zu erfassen, wann welche Person den Laden betreten und welches Produkt sie betrachtet hat.

Bei einer Einbindung solcher Elemente sind die Anforderungen des TTDSG (insbesondere § 25 TTDSG) und der DS-GVO (beispielsweise das Erfordernis einer Rechtsgrundlage) einzuhalten.

Nachfolgend sind Vorschläge aufgeführt, die eine **datenschutzfreundlichere** Einbindung von externen Inhalten auf Webseiten ermöglichen.

Unabhängig von den einzelnen Vorschlägen geht es allgemein darum, entsprechend der Artikel 24 ff. – insbesondere Artikel 25 und Artikel 32 DS-GVO – das Risiko für die Rechte und Freiheiten der betroffenen Personen durch die geplante Verarbeitung durch adäquate Maßnahmen zu verringern. Zu den Rechten und Freiheiten gehören z.B. die Rechtmäßigkeit und Transparenz der Verarbeitung, die Einhaltung der Vorgaben zu Übermittlungen an Drittländer und zur Informationssicherheit, die Wahrung der Vertraulichkeit, Verfügbarkeit und Integrität der Daten, die Zweckbindung und die Datenminimierung.

In diese Überlegung von „data protection by design“ können hierbei etablierte Ideen aus sog. „Privacy-Patterns“ oder „Privacy-enhancing technologies“ (PETS) einfließen<sup>6</sup>. Im Kontext von Webseiten können dies beispielsweise sein:

- **Lokale Verarbeitung:** Download der externen Inhalte durch den Webseiten-Betreiber und lokale Speicherung des einzubindenden Inhalts auf dem bereits genutzten Server des Webangebots.
- **Abwandlung:** Nutzung von Proxy-Skripten, die serverseitig den Aufruf beim Drittanbieter durchführen (z.B. Embetty).
- **Zwei-Klick-Lösung:** Nutzung von Vorschaltdialogen, die Inhalte erst nach Bestätigung laden (z.B. Shariff).

---

<sup>6</sup> Exemplarisch <https://privacybydesign.digital/>

## 2.1. Wie kann ich Social-Media-Buttons einbinden?

Wenn Sie ohne die oben dargestellte Problematik externe Verweise implementieren wollen, können Sie mit geeigneter optischer Gestaltung einen Link auf die Like- oder Share-Funktion der jeweiligen Plattform integrieren, bei dem kein externes Bild oder anderes Objekt geladen wird. Damit werden keine Daten an die jeweilige Plattform beim bloßen Aufruf der eigenen Seite übermittelt.

Alternativ lässt sich mit Hilfe des Projekts Shariff<sup>7</sup> der Fachzeitschrift c't sicherstellen, dass Social-Media-Buttons erst dann einen Kontakt mit dem jeweiligen Drittanbieter als Betreiber der Plattform herstellen, wenn der Nutzende aktiv die Vorschaltseite geklickt hat.

## 2.2. Wie kann ich externe Inhalte von Twitter, YouTube, Facebook und Co. einbinden?

Bei der direkten Einbindung von Inhalten wie Tweets von Twitter, Beiträgen auf Facebook oder YouTube-Videos werden wie dargestellt stets personenbezogene Daten und oftmals auch die genaue Identität der jeweiligen Nutzer\_innen an diese Dienste übermittelt.

Über eine sogenannte Zwei-Klick-Lösung (z. B. Embetty<sup>8</sup> der c't) lassen sich externe Inhalte von sozialen Medien so einbetten, dass zunächst nur eine Vorschau der externen Inhalte angezeigt wird – ohne dabei die IP-Adresse, Browser-Informationen oder andere persönliche Informationen an den Drittanbieter zu übermitteln. Erst wenn der Besucher aktiv auf die Vorschau klickt, um zum Beispiel ein YouTube-Video tatsächlich anzusehen, werden Daten übermittelt.

Bedenken Sie, dass betroffene Personen auch über die mit der Einbindung externer Medien einhergehenden Verarbeitungen personenbezogener Daten informiert werden müssen. Das bedeutet, dass den Nutzer\_innen vor Beginn des Abspielens verständlich gemacht werden muss, dass beispielsweise beim Abspielen eines eingebetteten YouTube-Videos die Information, wer welche Webseite gerade aufgerufen hat, an YouTube übermittelt wird und eine Verkettung mit bereits beim Drittanbieter vorhandenen Daten möglich ist. Häufig ist es auch gar nicht notwendig, Inhalte bzw. Medien wie Bilder oder Videos aus externen Quellen einzubinden bzw. nachzuladen. Die nachfolgenden Vorschläge können eine Zwei-Klick-Lösung obsolet machen:

- **Inhalte (z. B. Tweets von Twitter):** Externe Inhalte wie Tweets lassen sich ebenfalls als Screenshot/Bildschirmfoto oder textliches Zitat (mit Quellenangabe) in eine Website einbinden. Dies hat auch den Vorteil, dass die zitierten Inhalte weiterhin erhältlich sind, wenn Twitter oder der Autor die entsprechenden Tweets entfernt oder sperrt. Daher sollten Verantwortliche darauf verzichten, Tweets direkt über Twitter einzubinden und eine Übermittlung personenbezogener Daten der Leser\_innen an Twitter unterlassen.

---

<sup>7</sup> vgl. <https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html>

<sup>8</sup> vgl. <https://www.heise.de/newsticker/meldung/Embetty-Social-Media-Inhalte-datenschutzgerecht-einbinden-4060362.html>

Wenn Verantwortliche auf die Übermittlung personenbezogener Daten an Anbieter wie Twitter durch Einbettung von dortigen Inhalten nicht verzichten wollen, sind alle Bedingungen für solche Übermittlungen einzuhalten und alle notwendigen Informationen bereitzustellen.

- **Externe Medien (z. B. YouTube-Videos):** Anstatt ein Video aus einer externen Quelle wie YouTube einzubinden, kann die Auslieferung auch direkt über die eigene Webpräsenz erfolgen – sofern genug Speicherplatz und Bandbreite zur Verfügung steht. Alternativ kann auf eine externe Videoquelle auch ohne Einbindung einfach verlinkt werden.

### 2.3. Wie kann ich (externe) Kartendienste einbinden?

Um jemanden über den Standort eines Unternehmens, Vereins bzw. einer Institution zu informieren, werden häufig externe Kartendienste wie Google Maps in die Website eingebunden.

Vorbehaltlich weiterer Einschränkungen, beispielsweise aufgrund Drittstaatentransfers, ist auch hier eine Zwei-Klick-Lösung erforderlich, welche die Nutzenden transparent über die Verarbeitungen und Übermittlungen informiert, bevor persönliche Informationen an den Betreiber solcher Kartendienste übermittelt werden.

Als datenschutzfreundliche Alternative steht z. B. der Kartendienst Maps4BW des Landesamts für Geoinformation und Landentwicklung Baden-Württemberg zur Verfügung – allerdings ist der Dienst auf Baden-Württemberg beschränkt. Über das Geoportal BW<sup>9</sup> ist das Kartenmaterial online abrufbar.

Eine weitere Alternative, die eine datenschutzkonforme Einbindung von Kartenmaterial ermöglicht, ist die Einbindung von OpenStreetmap über eine Proxy-Lösung.<sup>10</sup> Für größere Organisationen kann sich auch der Betrieb eines kompletten OpenStreetmap-Servers bzw. eine lokale Speicherung der OpenStreetmap-Kacheln/Tiles lohnen. Da mit dieser Methode keine Daten an Dritte übermittelt werden, kann die Lösung grundsätzlich datenschutzkonform genutzt werden.

### 2.4. Wie kann ich (externe) Schriftarten/Fonts einbinden?

Um das gewünschte Aussehen einer Webseite zu erreichen, binden Anbieter von Telemediendiensten oft externe Schriftarten ein. Die Einbindung von externen Schriftarten bedingt allerdings eine Übermittlung personenbezogener Daten wie der IP-Adresse an den Anbieter. Eine Einbindung bzw. Auslieferung von Schriftarten kann demgegenüber auch lokal über die eigene Website erfolgen.

Besonders beliebt sind die kostenlos nutzbaren Schriftarten „Google Fonts“: Google hat ein Verzeichnis mit aktuell über 1300 Schriftarten verschiedener Designer, die unter einer freien Lizenz zur Verfügung stehen, zusammengestellt und bietet eine einfache Möglichkeit der Einbindung der Schriftarten in die eigene Webseite an. Auch eine solche Einbindung geht mit einer Übermittlung personen-

---

<sup>9</sup> Geoportal BW, siehe <https://www.geoportal-bw.de/>

<sup>10</sup> z.B. über die unter <https://dr-dsgvo.de/interaktive-karte-demo/> vorgestellte Datenschutzfreundliche Interaktive Karte oder andere ähnliche Implementierungen.

bezogener Daten an Google einher. Um dies zu vermeiden, können Webseitenbetreiber die Schriftarten auch problemlos vom eigenen Webspaces ausliefern. Die Auslieferung durch Google bringt heutzutage auch keine Caching-Vorteile mehr mit sich, da in der Zwischenzeit alle gängigen Browser aus Sicherheitsgründen keinen gemeinsamen Cache mehr für verschiedene Webseiten verwalten.

Eine einfache Möglichkeit die lokale Einbindung zu erreichen und die gewünschten Schriftarten aus dem Angebot der Google Fonts für den lokalen Einsatz zusammenzustellen bietet der Google Web Fonts Helper.<sup>11</sup>

## 2.5. Was muss bei Anbietern beachtet werden, die Daten außerhalb der EU übermitteln (Drittstaatentransfer)?

Die Regelungen von Kapitel 5 der DS-GVO sind bei der Übermittlung personenbezogener Daten in Drittländer zusätzlich zu beachten. Werden die Bedingungen aus Artikel 44 ff. DS-GVO nicht eingehalten, ist die Nutzung des jeweiligen Dienstes auch mit Einwilligung nicht zulässig und Anbieter von Webseiten müssen diese Übermittlungen einstellen.

Weitere Informationen zum Drittstaatentransfer finden sich in der Orientierungshilfe *Was jetzt in Sachen internationaler Datentransfer?* des LfDI BW.<sup>12</sup>

Dies betrifft auch das bei vielen Anbietern beliebte Google Analytics. Nach derzeitigem Stand (Februar 2022) haben sowohl die Datenschutz-Aufsichtsbehörden in Österreich<sup>13</sup> als auch in Frankreich<sup>14</sup> festgestellt, dass die von den jeweiligen Webseitenbetreibern getroffenen Maßnahmen zum Schutz personenbezogener Daten nicht ausreichend sind.

## 3. Reichweitenanalyse

Viele Webseitenbetreiber möchten analysieren, welche Inhalte des Internet-Angebots besonders häufig gelesen werden, welche Fehler auftreten oder an welcher Stelle die Besucher die Seite verlassen. Dieses Interesse ist grundsätzlich nachvollziehbar, das heutzutage oftmals übliche Vorgehen für eine solche Analyse birgt allerdings einige Fallstricke. Zu grundlegenden Fragen in Bezug auf den Begriff sowie datenschutzrechtlichen Fragen in diesem Kontext ist die OH Telemedien 2021 (Seite 24 f.) heranzuziehen.

Eine Reichweitenanalyse ist vom Tracking insoweit abzugrenzen, als das Ziel der Verarbeitung die Erstellung von nicht-personenbezieharen aggregierten Statistiken darstellt. Eine Erhebung von Daten mittels Wiedererkennung einzelner Nutzer\_innen über einen längeren Zeitraum kann nicht mehr

---

<sup>11</sup> siehe <https://google-webfonts-helper.herokuapp.com/fonts>

<sup>12</sup> Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer? – <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf>

<sup>13</sup> vgl. Bescheid der Österreichischen Datenschutzbehörde: <https://www.dsb.gv.at/dam/jcr:c1eb937b-7527-450c-8771-74523b01223c/D155.027%20GA.pdf>

<sup>14</sup> vgl. Meldung der CNIL: <https://www.cnil.fr/en/use-google-analytics-and-data-transfers-united-states-cnil-orders-website-manageroperator-comply>

als Reichweitenanalyse verstanden werden. Erhobene Daten über das Verhalten einzelner Nutzer sind für eine Reichweitenanalyse zum frühestmöglichen Zeitpunkt von einem Personenbezug zu befreien und werden in einer Statistik weiterverarbeitet.

Für die datenschutzrechtliche Gesamtbewertung ist nicht nur heranzuziehen, welche Statistiken dem Verantwortlichen üblicherweise angezeigt werden, sondern auch, welche Daten zur Darstellung gespeichert und anderweitig verarbeitet werden, ob weitere Verarbeitungen z.B. im Interesse Dritter vorgenommen werden oder ob Drittanbieter personenbezogene Daten verarbeiten.

### 3.1. Darf ich Werkzeuge zur Reichweitenanalyse ohne Einwilligung der Nutzenden verwenden?

Der Einsatz einer Reichweitenanalyse geht oftmals mit der Speicherung von Cookies oder dem Auslesen von Informationen des Endgeräts einher, um Nutzende anhand bestimmter Merkmale wiederzuerkennen. Nach § 25 Absatz 1 Satz 1 TTDSG erfordert solch eine Speicherung bzw. der Zugriff auf Informationen auf dem Endgerät eine **ausdrückliche, informierte, freiwillige, aktive und vorherige** Einwilligung der Nutzenden, da die genannten Ausnahmen nicht einschlägig sind. Diese Einwilligungspflicht gilt unabhängig davon, ob die auf den Endgeräten gespeicherten oder aus diesen ausgelesenen Informationen personenbezogen sind oder nicht.

Im folgenden Beispiel wird ein gestaltender Umgang mit den Anforderungen des TTDSG und der DSGVO exemplarisch dargestellt:

a)

Ziel im **Beispiel** ist eine Reichweitenanalyse, ohne dass nach dem TTDSG (da kein „Zugriff“) eine Einwilligung erforderlich wäre. Hierbei können folgende Informationen z.B. mittels Logfile-Analyse erfasst werden:

- **Hostname (FQDN), der aufgerufen wird:** www.baden-wuerttemberg.datenschutz.de
- **IP-Adresse des anfragenden Rechners:** 203.0.113.123
- Datum und Uhrzeit des Zugriffs: Tag/Monat/Jahr: Uhrzeit
- **Art des HTTP-Requests:** GET
- **aufgerufene Datei:** /datenschutz/
- **HTTP-Statuscode:** 200
- **Webseite, von der aus der Zugriff erfolgt (Referrer-URL):** -
- **Verwendeter Browser und ggf. Betriebssystem des zugreifenden Rechners (User-Agent):** Mozilla/5.0 (Betriebssystem; Variante) Gecko/X Firefox/X

Unter § 25 TTDSG fällt nur ein „Zugriff“ auf Informationen, wenn dieser zielgerichtet erfolgt. Sowohl IP-Adresse als auch User-Agent sind Informationen, die der Browser automatisch beim Aufruf einer Website mitsendet, ohne dass dies der Anbieter des Telemediendienstes beeinflussen könnte.

Der Server hat (anders als bei einem Cookie) keine Informationen als Wiedererkennungsmerkmal des Nutzenden auf dessen Endgerät gespeichert und er greift auch nicht auf Informationen „zu“ (oder initiiert einen Zugriff). Die Informationen wurden ohne Zutun des Anbieters des Telemediendienstes an ihn gesandt. Dieses Vorgehen wird demnach nicht vom § 25 TTDSG erfasst. Gleichwohl sind alle (weiteren) Verarbeitungen sehr wohl an den Maßstäben der DS-GVO zu messen.

Klarstellend ist zu ergänzen, dass bei einer Beeinflussung der übertragenen Informationen – sog. aktives Fingerprinting – beispielsweise mittels über JavaScript-Befehle abgerufener Informationen zu Bildschirmauflösung oder der Liste der installierten Schriftarten oder einer Änderung der bei einer mobilen Anwendung im HTTP-Header an den Server übertragenen Werte (z.B. veränderter User-Agent) ein „Zugriff“ vorliegt und die Anforderungen aus § 25 TTDSG deshalb einzuhalten sind.

b)

Die Verarbeitung der personenbezogenen Daten unterliegt den Anforderungen der DS-GVO. Hier ist zu überlegen, welche Rechtsgrundlage einschlägig ist. Denkbar ist, dass unter gewissen Umständen für die personenbezogene Verarbeitung anhand des erlangten Fingerprints (anhand obiger zugesandter Informationen) beispielsweise ein berechtigtes Interesse (Artikel 6 Absatz 1 Buchstabe f DS-GVO) eine Rechtsgrundlage darstellen könnte.

Um die Grenzen der Abwägung zwischen berechtigtem Interesse des Verantwortlichen und Gegeninteresse der betroffenen Person nicht zu überschreiten, ist eine Abwägung anhand der Kriterien der OH Telemedien 2021 (vgl. dort Seite 30 f.) sowie der Kriterien der OH Telemedien 2019<sup>15</sup> (vgl. dort Seite 11 ff.) durchzuführen:

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

Ein Nachteil aus Datenschutzsicht für den Nutzenden ist, dass er – anders als bei der Wiedererkennung mittels auf seinem Gerät gespeicherter Cookies – selbst das Wiedererkennungsmerkmal nicht mehr auf seinem Gerät löschen kann, sondern hierfür auf Funktionen zur Löschung des Wiedererkennungsmerkmals (und seinem damit einhergehenden „Steckbrief“) auf dem Server des Anbieters angewiesen ist und diese auf der Webseite auffinden muss.

In der Regel ermöglicht die Beachtung der nachfolgenden Punkte eine Reichweitenanalyse ohne Einwilligung:

- Reichweitenanalyse mittels lokaler Logfile-Analyse
- Verzicht auf Dienste externer Dritter
- Datensparsame Konfiguration
- Kein Zusammenführen von Nutzungsdaten (z.B. über Anbieter- oder Gerätegrenzen)
- Keine Verwendung der zur Wiedererkennung des Nutzenden erlangten Informationen für andere Zwecke.

Aus Sicht des Landesbeauftragten ist somit bei Einhaltung von gewissen Vorgaben der Einsatz einer Reichweitenanalyse nach TTDSG und DS-GVO ohne Einwilligung der Nutzenden möglich.

---

<sup>15</sup> Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, Version von 2019, abrufbar unter [https://www.datenschutzkonferenz-online.de/media/oh/20190405\\_oh\\_tmg.pdf](https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf)

Ansonsten ist regelmäßig eine Einwilligung in die konkrete Datenverarbeitung erforderlich (vgl. Seite 9 ff. der OH Telemedien 2021). Eine **ausdrückliche, informierte, vorherige, freiwillige, aktiv und separat von anderen Erklärungen eingeholte Einwilligung** der Nutzenden ist insbesondere erforderlich, wenn Dritten die Möglichkeit gegeben wird, Nutzungsverhalten zu analysieren oder wenn personenbezogene Daten an Dritte weitergegeben werden. Letzteres findet üblicherweise bei der Einbindung externer Reichweitenanalyse-Tools statt. Es ist auch wichtig zu prüfen, ob ein **Auftragsverarbeitungsvertrag** oder ein **Vertrag über die gemeinsame Verantwortung** notwendig ist und ob eine **Datenübertragung in Länder außerhalb der Europäischen Union** erfolgt und rechtmäßig ist (vgl. Abschnitt A 2.5).

Bei der Einholung einer Einwilligung sind die später genannten Voraussetzungen zu erfüllen. Verantwortliche sollten sich daher gut überlegen, ob sie diesen Aufwand wirklich betreiben wollen oder auf einwilligungsbedürftige Verarbeitungen nicht besser ganz verzichten.

### 3.2. Was ist serverseitiges Tracking und kann ich damit Vorgaben des TTDSG oder der DSGVO umgehen?

Serverseitiges (Server-side) Tracking ist ein relativ neues Konzept,<sup>16</sup> welches vor dem Hintergrund der zunehmenden Regulierung im Telemedienbereich in jüngster Zeit verstärkt diskutiert wird. Vereinfacht dargestellt ist die Idee dahinter, das Tracking vom Endgerät des Nutzenden auf den Server des Verantwortlichen auszulagern, der ohnehin den gesamten Traffic einer Website einsehen kann. Dort werden Daten dann gezielt gesammelt und aufbereitet und – im besten Fall in anonymisierter Form – an den Tracking-Dienstleister abgegeben, welcher seinerseits die gewünschten Analysen durchführt.

Selbstverständlich müssen auch beim serverseitigen Tracking die Anforderungen des TTDSG und – da es sich bei der Übermittlung personenbezogener Daten um eine Verarbeitung handelt – der DSGVO eingehalten werden.

So ist denkbar, dass der Anbieter des Telemediendienstes auf Informationen des Endgeräts des Nutzenden zugreift oder darin speichert, diese an den Server des Anbieters übertragen werden und dann serverseitig personenbezogene Daten an den Drittanbieter übermittelt werden.

Vorteile:

- Der offenkundige Vorteil für den Anbieter des Telemediendienstes ist, dass dann weder Cookies von Dritten noch Serververbindungen zu Dritten erforderlich sind und es damit keine direkte Verbindung zum Tracking-Dienstleister inkl. einer zwingenden Übermittlung einer IP-Adresse des Betroffenen gibt.
- Zusätzlich besteht für den Anbieter des Telemediendienstes die Möglichkeit, die Weitergabe von Daten und evtl. zu treffende Re-Pseudonymisierungen oder Anonymisierungen selbst zu bestimmen und damit die Risiken einer Verarbeitung maßgeblich zu senken.

---

<sup>16</sup> vgl. auch Schaubilder auf <https://www.basicthinking.de/blog/2022/02/02/affiliate-marketing-2022-daten-schutz-und-tracking/>

- Bei der Einbindung der von Drittanbietern zur Verfügung gestellten Code-Snippets durch den Anbieter des Telemediendienstes besteht für den Anbieter das Risiko, dass ihm die dortigen Programmabläufe nicht klar sind und bei externer Einbindung die Inhalte der Skripte vom Drittanbieter ausgetauscht werden können. Daneben laufen die Skripte bei Einbindung mittels `<script>` im Kontext der Webseite und sind im Regelfall nicht durch ein `<iframe>` isoliert, was ein Sicherheitsrisiko darstellen kann. Dieses Risiko entfällt, wenn keine Skripte in die Webseite eingebunden werden.
- Eines der wesentlichen Risiken der direkten Einbindung von Tracking-Dienstleistern, nämlich die Website-übergreifende Nachverfolgung des Verhaltens Einzelner, ist mit einem Server-side-Tracking und geeigneten Schutzmaßnahmen deutlich besser kontrollierbar als mit herkömmlichen Tracking-Methoden.

### Nachteile:

- Für die betroffenen Personen besteht das Risiko, dass die serverseitigen Verbindungen vom Nutzenden nicht mehr beobachtbar sind, deswegen vom Verantwortlichen auch heimlich durchgeführt werden könnten und die Transparenz der Datenverarbeitung (vgl. Artikel 5 Absatz 1 Buchstabe a DS-GVO) leidet.
- Denkbar ist auch, dass der Verantwortliche zusätzliche Informationen (z.B. durch Ergänzung mit weiteren Informationen aus einem Nutzer\_inaccount) mit an den Dritten überträgt, was der Nutzende nicht selbst nachvollziehen kann.
- Für den Anbieter besteht das Risiko, dass eine vom Drittanbieter zur Verfügung gestellte Software zur serverseitigen Übertragung unklare Programmabläufe enthält, die auf dem Server ausgeführt werden.

Findet ein Server-Side-Tracking ohne Cookies (einschließlich aus anderen Gründen vorhandener Cookies) statt und werden Nutzungsdaten vor einer Weitergabe an einen Tracking-Dienstleister vollständig anonymisiert, dann kann diese Verarbeitung ggf. auf ein berechtigtes Interesse nach Artikel 6 Absatz 1 Buchstabe f DS-GVO gestützt werden und eine Anwendung des TTDSG scheidet aus. Es ist zu beachten, dass das bloße Ersetzen von Identifizierungsmerkmalen durch andere wie User-IDs oder Hashes (vgl. auch OH Telemedien 2019, Seite 15) **keine** Pseudonymisierung und auch keine Anonymisierung darstellt. Wenn z.B. Nutzer\_innenpfade individualisiert werden und diese Individualisierung über eine Session hinausgeht, liegt ebenso keine Anonymisierung vor. Zudem kommt es darauf an, ob Cookies genutzt werden oder ob ein Fingerprinting von Nutzer\_innen z.B. mittels Auslesen von installierten Schriftarten via JavaScript stattfindet. In diesen Fällen ist der Anwendungsbereich des TTDSG eröffnet. Werden identifizierende Merkmale verarbeitet bzw. an den Tracking-Dienstleister weitergegeben, ist auch der Anwendungsbereich der DS-GVO eröffnet und die konkreten Risiken der Verarbeitung müssen betrachtet werden, beispielsweise ob trotz aller getroffenen Maßnahmen nicht ausgeschlossen werden kann, dass ein Tracking-Dienstleister mit eigenen Mitteln und dem vorliegenden Datenbestand eine Re-Identifizierung einer betroffenen Person durchführen kann. Dieses Risiko ist aufgrund der teilweise gewaltigen Datenbestände und der hohen Marktdurchdringung großer Tracking-Dienste-Anbieter nicht unerheblich.

## 4. Anforderungen an Einwilligungs-Banner

Die rechtskonforme Gestaltung von Einwilligungs-Bannern ist eine große Herausforderung und im Einzelfall von den konkreten Verarbeitungen, in die eingewilligt werden soll, abhängig. **Daher ist es für Verantwortliche deutlich einfacher und risikoärmer, auf einwilligungsbedürftige Verarbeitungen ganz zu verzichten.**

Neben den im Folgenden aufgeführten Punkten sind auch die Hinweise in der OH Telemedien sowie der einschlägigen Leitlinien des Europäischen Datenschutzausschusses zu beachten, insbesondere die Leitlinien zur Einwilligung<sup>17</sup> und die Leitlinien zu datenschutzfreundlichen Voreinstellungen.<sup>18</sup>

### 4.1. Auf welchen Unterseiten sind Einwilligungs-Banner erforderlich?

Viele Webseiten führen nur auf einzelnen speziellen Unterseiten einwilligungsbedürftige Verarbeitungen (einschließlich des Setzens oder Auslesens von Cookies) durch. Dann ist es nicht notwendig und sinnvoll, bereits auf der Startseite oder auf jeder Seite eines komplexen Internet-Angebots eine Einwilligung einzuholen. Es sollten nur dort Einwilligungen eingeholt werden, wo dies auch notwendig ist. Auch vor dem Hintergrund des Transparenzgebots sollten Einwilligungen nur dann eingeholt werden, wenn sie notwendig sind.

Das **Impressum** und die **Datenschutzinformationen** nach Artikel 13, 14 DS-GVO müssen stets ohne Behinderung durch einen Einwilligungsbanner oder ähnliches erreichbar sein.

### 4.2. Was sind die Anforderungen an die informierte, freiwillige, aktive und vorherige Einwilligung?

Das TTDSG enthält keine Vorgaben für die Einwilligung, sondern verweist in § 25 Absatz 1 Satz 2 TTDSG bezüglich der Informationspflichten gegenüber den Nutzenden als auch der formalen und inhaltlichen Anforderungen einer Einwilligung auf die DS-GVO.

Eine wirksame Einwilligung in die Speicherung/den Zugriff auf Informationen nach TTDSG und die geplante weitere Verarbeitung der ausgelesenen Daten gemäß Artikel 6 Absatz 1 Buchstabe a oder Artikel 9 Absatz 2 Buchstabe a DS-GVO kann unter Berücksichtigung von Bedingungen (vgl. Seite 9 ff. OH Telemedien 2021) grundsätzlich **gleichzeitig** eingeholt werden.

Eine Einwilligung ist nach ihrer Definition in Artikel 4 Nr. 11 DS-GVO nach eine „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“. Die betroffene Person muss die Verarbeitung, in die sie einwilligt, also wollen.

---

<sup>17</sup> Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679 des Europäischen Datenschutz-Ausschusses, siehe [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_de.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_de.pdf)

<sup>18</sup> Leitlinien 4/2019 zu Artikel 25, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Version 2.0, siehe [https://edpb.europa.eu/system/files/2021-04/edpb\\_guidelines\\_201904\\_data-protection\\_by\\_design\\_and\\_by\\_default\\_v2.0\\_de.pdf](https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_data-protection_by_design_and_by_default_v2.0_de.pdf)

Damit eine Einwilligung wirksam ist, sind mehrere Bedingungen einzuhalten:

- **Vorherigkeit:** Eine Verarbeitung darf erst nach Erteilung der Einwilligung erfolgen.
- **Freiwilligkeit:** Die betroffene Person muss aus freien Stücken und ohne Zwang einwilligen. Die Ablehnung darf nicht schwerer als die Erteilung der Einwilligung sein.
- **Informiertheit:** Über die Vorgänge und Verarbeitungen muss in transparenter Weise informiert werden.
- **Aktive Einwilligung:** Einwilligungen müssen aktiv von den betroffenen Personen abgegeben werden. Eine bloße Information vor oder parallel zum Weitersurfen ist nicht ausreichend.
- **Separat von anderen Erklärungen:** Einwilligungen müssen separat von anderen Erklärungen – beispielsweise der Zustimmung zu den AGB eines Online-Shops – abgegeben werden.
- **Widerruflichkeit:** Nutzende müssen ihre Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen können.

Im Text der Einwilligungserklärung (vgl. Seite 9 ff. der Orientierungshilfe) muss die Speicherung/der Zugriff auf Informationen (nach TTDSG) und der weitere Verarbeitungsvorgang (nach DS-GVO) klar und deutlich beschrieben werden. Nutzer\_innen müssen ohne weiteres verstehen können, worin sie einwilligen. Ein bloßer Hinweis „*diese Seite verwendet Cookies, um Ihr Surferlebnis zu verbessern*“ oder „*für Webanalyse und Werbemaßnahmen*“ ist nicht ausreichend, sondern irreführend, weil die damit verbundenen Verarbeitungen nicht transparent gemacht werden. Die Einwilligung muss nicht nur nach TTDSG für die Verwendung von Cookies an sich, sondern nach DS-GVO auch für die Verarbeitung personenbezogener Daten eingeholt werden. Insbesondere muss genau und verständlich aufgelistet werden, an welche namentlich zu benennenden Empfänger welche Daten weitergegeben werden, bzw. wer personenbezogene Daten verarbeitet, zu welchem Zweck dies geschieht und mit welchen anderen personenbezogenen Daten diese angereichert werden. Verfolgen Empfänger eigene Zwecke, müssen auch diese beschrieben werden. Diese Informationen müssen klar und deutlich in einfacher Sprache dargestellt werden und dürfen nicht versteckt oder verschleiert werden. Durch die Wahl der Überschrift wie „*Wir schätzen Ihre Privatsphäre*“ oder „*Wir lieben Kekse*“ darf keine Irreführung entstehen. Nutzer\_innen müssen aktiv und freiwillig einwilligen (Opt-In), die Zustimmung darf nicht vorausgewählt sein. Opt-Out-Verfahren oder bereits im Vorhinein angekreuzte Kästchen reichen nicht aus („*data protection by default*“). Das Ablehnen bzw. nicht Einwilligen muss genauso einfach wie das Einwilligen sein.

Über alle Vorgänge muss ausreichend und transparent informiert werden (Art. 5 Abs. 1 Buchstabe a, Art. 12 ff. DS-GVO), damit betroffene Personen eine bewusste eigenständige Entscheidung fällen können. Dabei ist es nicht ausreichend, nur das Ergebnis der Verarbeitung (z.B. Anzeige von Werbung) zu benennen, sondern es muss auch die Datenverarbeitung selbst (z.B. Erstellung eines Dossiers über die Interessen und Vorlieben der betroffenen Person durch Aufzeichnung, Nachverfolgung und Überwachung der Internet-Nutzung) in verständlicher Form beschrieben werden.

Die jeweiligen Empfänger sollten einzeln bzw. nach Kategorien auswählbar sein. Vor einer aktiven Einwilligung des Nutzenden dürfen keine Daten erhoben bzw. entsprechende Elemente nachgeladen werden. Auch das bloße (Fort-)Nutzen einer Website oder einer App stellt keine wirksame Einwilligungserklärung dar.

Freiwillig ist die Einwilligung nur, wenn die betroffene Person eine echte oder freie Wahl hat (vgl. Seite 15 ff. OH Telemedien 2021) und eine Einwilligung auch verweigern kann, ohne dadurch besondere Nachteile zu erleiden. Eine Koppelung einer vertraglichen Dienstleistung an die Einwilligung zu einer für die Vertragserbringung nicht erforderlichen Datenverarbeitung führt regelmäßig dazu, dass die Einwilligung nicht freiwillig und damit unwirksam ist (vgl. Art. 7 Abs. 4 DS-GVO). Behörden und andere öffentliche Stellen können aufgrund Erwägungsgrund 43 DS-GVO üblicherweise keine wirksamen Einwilligungen einholen. Denn wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, soll die Einwilligung keine gültige Rechtsgrundlage liefern.

Öffentliche Stellen wie z.B. Behörden sollten deswegen grundsätzlich auf einwilligungsbedürftige Verarbeitungen und das Setzen und Auslesen von Informationen auf den Endgeräten der Nutzenden verzichten.

#### 4.3. Wie gestalte ich Einwilligungs-Banner?

Vor der Gestaltung eines sog. „Einwilligungs-Banners“ sollte zuerst geprüft werden, ob dieser erforderlich ist. Denn die Nutzung von Cookies sind nicht per se einwilligungsbedürftig – siehe A 1.1. Datenverarbeitungen (ob mit oder ohne Hilfe von Cookies), für die keine Einwilligung erforderlich ist, müssen nur in den **Datenschutzhinweisen** dargestellt werden. Einwilligungs-Banner müssen eingesetzt werden, wenn tatsächlich eine Einwilligung des Nutzenden nötig ist, also z.B. beim Einsatz technisch nicht erforderlicher Cookies oder bei der Weitergabe von Daten an Dritte.

Sofern eine Einwilligung erforderlich ist, hat diese Abfrage unmittelbar vor der ersten Nutzung der einwilligungsbedürftigen Funktionalität z.B. in Form eines Banners oder ähnlich gestaltetem Element (beispielsweise grafischen Schaltflächen) zu erfolgen. Folgende Anforderungen (vgl. auch Seite 28 ff. OH Telemedien 2021) gilt es bei der Gestaltung eines Einwilligungs-Banners zu beachten:

- **Deutlich und verständlich:** Klare, **nicht irreführende Überschrift** – bloße Respektbekundungen bezüglich der Privatsphäre reichen nicht aus. Es empfehlen sich Überschriften, in denen auf die Tragweite der Entscheidung eingegangen wird, wie beispielsweise „Weitergabe Ihrer Nutzerdaten an Dritte zur Ermittlung Ihrer Interessen“.
- **Zweck der Verarbeitung:** Der **Gegenstand** der Einwilligung muss **deutlich gemacht** werden – **klare Beantwortung der folgenden Fragen:** Welche personenbezogenen Daten sind betroffen? Was passiert mit ihnen? Wer erhält Zugriff auf die Daten? Werden die personenbezogenen Daten mit weiteren Daten verknüpft? Welchen Zwecken dient das?
- **Datenschutzfreundliche Voreinstellung:** Die Einwilligung darf nicht voreingestellt sein – ein **Opt-in** ist notwendig.
- **Keine vorherigen (Dritt-)Verbindungen:** Es dürfen **keine Daten weitergegeben** werden, **bevor eine Einwilligung** durch den Nutzenden erteilt wurde. Das bedeutet: Technisch muss sichergestellt sein, dass während der Einwilligungs-Banner angezeigt wird, keine weiterführenden (Tracking-)Skripte ausgeführt werden und/oder nicht notwendige Cookies im Browser abgelegt werden.

- **Keine Manipulation (Nudging):** Nutzer\_innen dürfen nicht unterschwellig zur Abgabe einer Einwilligung beeinflusst werden. Das ist beispielsweise dann der Fall, wenn Buttons/Schaltflächen durch eine farbliche Hervorhebung, Größe oder Position deutlich auffälliger gestaltet sind. Auf Nudging, also die Beeinflussung des Nutzenden, um sein/e Entscheidung zu manipulieren, soll verzichtet werden.
- **Einfach zugängliche Ablehnung:** Bereits auf der ersten Ebene muss es möglich sein, dem Ablegen von Cookies bzw. dem Zugriff auf Informationen auf dem Endgerät zu widersprechen. Nicht Einwilligen muss genauso einfach sein wie Einwilligen. Zum Hintergrund: Oftmals ist die Verweigerung erst auf Ebene zwei (oder drei) bzw. über mehrere Klicks erreichbar. Wie auch bei der Einwilligung muss dem Nutzenden eine einfache Möglichkeit angeboten werden, der Verarbeitung seiner Daten zu widersprechen.
- **Erreichbarkeit Datenschutzerklärung / Impressum:** Der **Zugriff auf Impressum und Datenschutzhinweise** darf nicht verhindert oder eingeschränkt werden, bevor eine Einwilligung durch den Nutzenden erteilt wurde.
- **Freiwilligkeit der Einwilligung:** Die **Freiwilligkeit** der Einwilligungserklärung muss deutlich gemacht werden und ein Hinweis auf das Recht auf einen **jederzeitigen Widerruf** muss enthalten sein (Art. 7 Abs. 3 Satz 3 DS-GVO); beispielsweise „Diese Einwilligung ist freiwillig, sie stellt keine Bedingung für die Nutzung dieser Website dar und kann jederzeit widerrufen werden, indem [...]“.
- **Widerrufsmöglichkeit:** Wie der Widerruf zu erklären ist, ist in der Information zur Einwilligungserklärung klar und deutlich zu beschreiben. Die **Erklärung des Widerrufs** muss jederzeit so einfach sein wie die Einwilligungserklärung selbst (Art. 7 Abs. 3 Satz 4 DS-GVO).

#### 4.4. Welche Informationen müssen in Einwilligungsbannern zum Zweck gegeben werden?

Es muss über den Zweck der jeweiligen Verarbeitungen personenbezogener Daten transparent, in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache informiert werden (Art. 12 Abs. 1 DS-GVO), damit Nutzer\_innen sich bewusst und informiert dafür oder dagegen entscheiden können, dieser Verarbeitung zuzustimmen oder nicht. Es darf nicht über den wahren Zweck der Datenverarbeitung getäuscht werden. Dabei sind nicht nur der Zweck des Seitenbetreibers zu nennen, sondern auch die Zwecke, für die ein Empfänger der Daten diese verwendet. So ist die Angabe „Anzeige von Werbung“ nicht ausreichend, wenn in Wahrheit der Zweck die Erstellung und der Verkauf personenbezogener Dossiers über Verhaltensbeobachtung, persönliche Vorlieben, politische Meinungen oder die sexuelle Orientierung an beliebig viele Dritte ist.

Es ist nicht ausreichend, nur das Ergebnis der Verarbeitung zu benennen, sondern die Datenverarbeitung an sich muss in einer klaren und einfachen Sprache beschrieben werden. Der Betreiber eines Internet-Angebots ist in der Pflicht, auch die Verarbeitungen seiner Partner transparent darzustellen.

#### 4.5. Können Standards der Werbeindustrie zum Einholen von Einwilligungen bedenkenlos verwendet werden?

**Nein.** Standards der (Werbe-)Industrie müssen zwar den Vorgaben der DS-GVO entsprechen. Diese halten sie aber nicht immer ein. So hat die Belgische Datenschutz-Aufsichtsbehörde mit Entscheidung vom 2. Februar 2022 (Fall-Nummer DOS-2019-01377)<sup>19</sup> festgestellt, dass das häufig verwendete Transparency Consent Framework (TCF) des Interactive Advertising Bureau Europe (IAB Europe) gegen die DS-GVO verstoße. Die Nutzung solcher Standards oder von Einwilligungs-Bannern spezialisierter Anbieter geht nicht per se mit einer rechtskonformen Implementierung einher.

#### 4.6. Was muss bei Gesundheitsdaten, Daten zur sexuellen Orientierung, politischen Meinungen und anderen besonderen Kategorien personenbezogener Daten beachtet werden?

Die Verarbeitung besonderer Kategorien personenbezogener Daten<sup>20</sup> ist grundsätzlich verboten und nur unter den engen Voraussetzungen aus Artikel 9 Absatz 2 DS-GVO erlaubt. Im Bereich Tracking kommt dabei nur die **ausdrückliche** Einwilligung der Nutzer\_innen in Frage.

Dies bedeutet erhöhte Anforderungen gegenüber der ‚normalen‘ Einwilligung. So muss den Nutzenden in transparenter Weise dargelegt werden, dass diese Daten verarbeitet werden und ihr ausdrücklicher Wille dazu abgefragt werden.

#### 4.7. Können jegliche Verarbeitungen durchgeführt werden, wenn eine wirksame Einwilligung eingeholt wurde?

**Nein.** Die sonstigen Vorschriften der DS-GVO sind ebenfalls zu beachten. Wenn Verarbeitungen und Geschäftsmodelle nicht mit der DS-GVO vereinbar sind, können diese auch nicht rechtmäßig eingesetzt werden. Dabei ist insbesondere Artikel 5 DS-GVO wichtig: Personenbezogene Daten dürfen demnach nur verarbeitet werden, wenn die Grundsätze „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“ sowie „Integrität und Vertraulichkeit“ eingehalten und deren Einhaltung vom Verantwortlichen – also z.B. dem Betreiber eines Internetangebots – nachgewiesen werden können (Rechenschaftspflicht, Artikel 5 Absatz 2 DS-GVO). Siehe auch das in Abschnitt 4.5 dargestellte Beispiel.

---

<sup>19</sup> für eine englische Übersetzung der Entscheidung siehe <https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-21-2022-english.pdf>

<sup>20</sup> Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Vgl. Artikel 9 Absatz 1 DS-GVO.

## Abschnitt B: Negativbeispiele und „Standardfehler“

Dieser Abschnitt enthält Beispiele für typische Fehler, die von Anbietern von Internetangeboten und anderen Telemediendiensten häufig gemacht werden, insbesondere bei der Einholung von Einwilligungen und der Gestaltung von Einwilligungs-Bannern. Die Fülle an Fehlerquellen zeigt die Größe der Herausforderung, vollständig rechtskonforme Einwilligungen einzuholen. Es empfiehlt sich daher schon aus Gründen der Risikominimierung, auf einwilligungsbedürftige Verarbeitungen soweit möglich zu verzichten.

### 1. Einhaltung der Bedingungen für wirksame Einwilligungen

Damit Einwilligungen wirksam sind, müssen sie verschiedene Anforderungen erfüllen. Die Bedingungen sind in Kapitel A. 4.2 genauer erläutert. In der Praxis sind die folgenden Fehler häufig anzutreffen:

#### 1.1. Vorherige Einwilligung

Eine einwilligungsbedürftige Verarbeitung (einschließlich des Setzens und Auslesens von Cookies) darf erst nach Erteilung einer Einwilligung erfolgen. Nachfolgende typische Fehler verstoßen gegen die Bedingung „*vorherig*“:

- 1.1.1. Die Datenverarbeitung beginnt bereits oder es werden Cookies genutzt, bevor eine notwendige Einwilligung erklärt wurde, insbesondere...
  - 1.1.1.1. ... sofort bei Aufruf der Website,
  - 1.1.1.2. ... noch während der Navigation auf das Impressum oder die Datenschutz-Informationen nach Art. 12 ff. DS-GVO.

#### 1.2. Freiwillige Einwilligung

Die betroffene Person muss aus freien Stücken und ohne Zwang einwilligen. Freiwilligkeit bedeutet dabei, dass die betroffene Person eine freie Wahl hat und sich ohne unzumutbaren Druck entscheiden kann. Die Ablehnung darf dabei nicht schwerer gemacht werden als die Erteilung der Einwilligung. Nachfolgende typische Fehler verstoßen gegen die Bedingung „*Freiwilligkeit*“:

- 1.2.1. Die Erklärung der Einwilligung ist vorausgewählt oder „Weitersurfen“ bzw. Anklicken eines Link wird als Einwilligung interpretiert (vgl. Erwägungsgrund 32 Satz 3 DS-GVO; EuGH, Urteil vom 1.10.2019 – C-673/17 – Planet 49).
- 1.2.2. Nicht Einwilligen ist schwerer oder zeitintensiver als Einwilligen.
- 1.2.3. Ablehnung ist nur mit unverhältnismäßigem Aufwand möglich, z.B.
  - 1.2.3.1. ... erfordert sie die Installation einer Software oder eines Browser-Plugins,
  - 1.2.3.2. ... erfordert sie die Konfiguration des Endgerätes oder Browsers.
- 1.2.4. Es wird versucht eine Einwilligung einzuholen, obwohl diese in der Verarbeitungssituation grundsätzlich nicht wirksam ist, z.B. weil ...

- 1.2.4.1. ... es sich beim Verantwortlichen um eine Behörde handelt (vgl. Erwägungsgrund 43 DS-GVO)
- 1.2.4.2. ... die Erfüllung eines Vertrages an die Abgabe einer Einwilligung gekoppelt ist (vgl. Artikel 7 Absatz 4 DS-GVO).
- 1.2.5. Durch die Gestaltung der Seite sind bei gängigen Bildschirmauflösungen ablehnende Bedienelemente nicht erreichbar.

### 1.3. Informiertheit

Über die Vorgänge und Verarbeitungen muss in präziser, transparenter, verständlicher Weise in einer klaren und einfachen Sprache informiert werden. Nachfolgende Fehler verstoßen gegen die Bedingung „*Informiertheit*“:

- 1.3.1. Die Information ist nicht in deutscher Sprache abgefasst, zielt aber auf deutsches Publikum.
- 1.3.2. Die Information ist nicht zumutbar erreichbar, nämlich nicht ...
  - 1.3.2.1. ... zeitlich vor der Abgabe der Einwilligungserklärung **und**
  - 1.3.2.2. ... jederzeit nach Abgabe der Einwilligungserklärung.
- 1.3.3. Die Information ist nicht zumutbar zur Kenntnis zu nehmen, insbesondere durch ...
  - 1.3.3.1. ... ihre optische Gestaltung,
  - 1.3.3.2. ... Verweise zu weiteren Erklärungen, wobei z. B. bei einer Verlinkung auf eine andere Website dort häufig erneut getrackt wird,
  - 1.3.3.3. ... ihre übergroße Länge,
  - 1.3.3.4. ... ihre unüberschaubare Komplexität
- 1.3.4. Ein Einwilligungsbanner verweist nur auf umfangreiche Informationen nach Artikel 13 DS-GVO, ohne selbst ausreichend über die Verarbeitungen zu informieren.
- 1.3.5. Die Information ist unvollständig, z.B. indem ...
  - 1.3.5.1. ... nur darüber informiert wird, dass Cookies verwendet werden, aber nicht darüber, welche Verarbeitungen personenbezogener Daten erfolgen,
  - 1.3.5.2. ... nicht über alle Verarbeitungen informiert wird,
  - 1.3.5.3. ... nicht über alle Zwecke informiert wird,
  - 1.3.5.4. ... Verarbeitungen oder Zwecke nur beispielhaft erwähnt werden,
  - 1.3.5.5. ... keine oder unvollständige Informationen über die einzelnen Cookies gegeben werden,
  - 1.3.5.6. ... nicht alle verwendeten Techniken (z.B. Cookies, ETags, Fingerprinting, Web Storage, TLS-Session-IDs) vollständig aufgeführt werden,
  - 1.3.5.7. ... Fingerprinting verwendet wird, aber nicht alle dafür herangezogenen Quellen genannt sind.
- 1.3.6. Die Informationen erfolgen nicht vollständig, da nicht alle Quellen und Zusammenführungen von Daten genannt werden, z.B.
  - 1.3.6.1. ... Offline-Daten,
  - 1.3.6.2. ... andere Internet-Angebote,
  - 1.3.6.3. ... Zusammenführungen über Gerätegrenzen hinweg.

- 1.3.7. Die **Überschrift** eines Einwilligungsbanners ist missverständlich, für die Zwecke nicht angemessen, irreführend, falsch oder erweckt einen falschen Eindruck über das wahre Ausmaß der Verarbeitungen. Dies ist insbesondere der Fall, wenn die Überschrift nicht zu den Verarbeitungen passt, in die eingewilligt werden soll. Beispiele für grundsätzlich irreführende Überschriften für den Fall, dass in die **Weitergabe von Nutzungs- und Verhaltensdaten zur Erstellung personenbezogener Werbeprojekte** eingewilligt werden soll:
- 1.3.7.1. „Wir lieben Cookies“
  - 1.3.7.2. „Diese Webseite verwendet Cookies“ (obwohl umfangreiche Verarbeitungen oder Übermittlungen stattfinden)
  - 1.3.7.3. „Willkommen“
  - 1.3.7.4. „Ihre Privatsphäre ist uns wichtig“
  - 1.3.7.5. „Wir respektieren Ihre Privatsphäre“
  - 1.3.7.6. „Es ist uns ein Anliegen, Ihre Daten zu schützen“
  - 1.3.7.7. „Wir benötigen Ihre Zustimmung“
  - 1.3.7.8. „Weiter mit Werbung lesen“
  - 1.3.7.9. „Mit Liebe serviert“
  - 1.3.7.10. „Wir halten uns an die DS-GVO“
  - 1.3.7.11. „Wir schneiden hier alles auf dich zu“
  - 1.3.7.12. „Ein Klick für den Datenschutz“
  - 1.3.7.13. „Diese Webseite mit Werbung und Cookies nutzen“
  - 1.3.7.14. „Cookies zustimmen“
  - 1.3.7.15. „Bevor Sie zum Inhalt weitergehen“
  - 1.3.7.16. „Ihr bestmögliches Nutzererlebnis“
  - 1.3.7.17. „Helfen Sie uns mit Ihrer Zustimmung“
- 1.3.8. Die Information ist inhaltlich falsch, insbesondere weil ...
- 1.3.8.1. ... über den Zweck der Datenverarbeitung getäuscht wird (z.B. „Anzeige von Werbung“ statt in Wahrheit „Verkauf personenbezogener Dossiers über Verhaltensbeobachtung an beliebige und beliebig viele Dritte“),
  - 1.3.8.2. ... nur ein Ergebnis der Verarbeitung benannt, nicht aber die Datenverarbeitung selbst beschrieben wird,
  - 1.3.8.3. ... über das Ausmaß der Datenverarbeitung getäuscht wird, insbesondere wenn Verarbeitungen stattfinden, die nicht oder nur an versteckter Stelle genannt werden,
  - 1.3.8.4. ... statt über den Zweck über die technische Methode informiert wird (z.B. „Informationen auf einem Gerät speichern und/oder abrufen“),
  - 1.3.8.5. ... Verarbeitungen genannt werden, die nicht stattfinden.  
... falsche oder irreführende Aussagen über die Eingriffsintensität der Verarbeitung gemacht werden,
  - 1.3.8.6. ... falsche oder irreführende Aussagen darüber gemacht werden, wie sensibel die verarbeiteten Daten sind.
- 1.3.9. Die notwendigen Informationen werden nicht in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache dargestellt.

- 1.3.10. Es findet keine ausreichende zusätzliche Information nach Artikeln 13, 14, 26 DS-GVO statt.
- 1.3.11. Die Information ist für den durchschnittlichen Nutzer unverständlich, etwa durch ...
  - 1.3.11.1. ... fremd- oder (pseudo-) fachsprachliche Begriffe (z.B. „Vendoren“, „Publisher“, „Prozessoren“, „Consent“, ...).
  - 1.3.11.2. ... Umdeutung von für durchschnittliche Benutzer bekannten oder anders zu verstehende Begriffe (z.B. „Wesentliche Dienste“).
  - 1.3.11.3. ... völlig unklare Struktur und Gestaltung.
- 1.3.12. Die Auswahlmöglichkeiten sind irreführend, insbesondere weil ...
  - 1.3.12.1. ... ein Bedienelement so gestaltet ist, dass sein Status quo und die Wirkung einer Nutzeraktion unklar bleibt. Bsp.: ein Button „Bestätigen“ lässt den Nutzer im Unklaren, ob der Wunsch des Websitebetreibers nach vollumfänglichem Tracking bestätigt wird oder die ggf. beschränkende Auswahl des Nutzers.
  - 1.3.12.2. ... durch die optische Gestaltung nicht klar ist, was ausgewählt ist und was nicht.
  - 1.3.12.3. ... das Betätigen eines Bedienelements zunächst zur Aktivierung der Einwilligung führt, die dann wieder durch weiteres Betätigen deaktiviert werden muss.
  - 1.3.12.4. ... ein Bedienelement so gegenüber anderen hervorgehoben ist, dass intuitiv dieses Element betätigt wird, was einer Vorauswahl wirkungsgleich ist. Bsp.: ein großer, grüner „OK“-Button wird leicht anklickbar präsentiert, ein kleiner Link auf „Einstellungen“ führt eher versteckt zu den Konfigurationsmöglichkeiten.

#### 1.4. Aktive Einwilligung

Einwilligungen müssen aktiv von den betroffenen Personen abgegeben werden. Eine bloße Information und das Weitersurfen sind nicht ausreichend. Nachfolgende Fehler verstoßen gegen die Bedingung „Aktive Einwilligung“:

- 1.4.1. Es ist nur ein Hinweis-Banner zu sehen, die einwilligungsbedürftigen Verarbeitungen beginnen aber schon ohne aktive Interaktion.
- 1.4.2. Es erscheint nur ein Hinweis-Banner mit Link zu weiteren Informationen, der nach einiger Zeit ausgeblendet wird.
- 1.4.3. Ein normales Nutzerverhalten wird fälschlicherweise als Erteilung einer Einwilligung interpretiert, z.B. ...
  - 1.4.3.1. ... Weiterscrollen.
  - 1.4.3.2. ... Schließen eines Banners.
  - 1.4.3.3. ... Klick neben einen Banner.
- 1.4.4. Verweis auf die Möglichkeit, Cookies im Browser zu löschen und im Browser Datenschutzeinstellungen zu treffen.

### 1.5. Separat von anderen Erklärungen

Einwilligungen müssen separat von anderen Erklärungen abgegeben werden. Der nachfolgende beispielhafte Fehler verstößt gegen die Bedingung „*Separate Erklärung*“:

- 1.5.1. Ein Online-Shop versteckt die datenschutzrechtliche Einwilligung in den AGB, denen beim Einkauf zugestimmt werden muss.

### 1.6. Widerruflichkeit

Nutzende müssen ihre Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen können. Nachfolgende Fehler verstoßen gegen die Bedingung „*Widerruflichkeit*“:

- 1.6.1. Es wird nicht mit der Einholung der Einwilligung darüber informiert, dass und wie die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen werden kann (Artikel 7 Absatz 3 Satz 3 DS-GVO).
- 1.6.2. Der Widerruf der Einwilligung ist durch die äußere oder sprachliche Gestaltung der Seite erheblich erschwert (Art. 7 Absatz 3 Satz 4 DS-GVO)
- 1.6.3. Der Widerruf der Einwilligung ist nicht so einfach wie die Erteilung der Einwilligung.
- 1.6.4. Einwilligung kann durch Mausklick erfolgen, aber der Widerruf ...
  - 1.6.4.1. ... ist nicht unmittelbar auf der Webseite möglich, sondern nur durch Brief, Anruf, Fax.
  - 1.6.4.2. ... erfolgt über ein umfangreiches Formular auf Webseite und damit i.d.R. datenintensiver
- 1.6.5. Verweis darauf, dass der Widerruf bei einem Drittdienst einzulegen ist
- 1.6.6. Es besteht keine zumutbare Möglichkeit, die Einwilligung zu widerrufen oder dem Widerruf wird keine Folge geleistet (Art. 7 Absatz 3 DS-GVO).

## 2. Rechtmäßigkeit, Fairness und Transparenz

Nach Artikel 5 Absatz 1 Buchstabe a DS-GVO müssen personenbezogene Daten auf rechtmäßige Weise nach „Treu und Glauben“ und für die betroffene Person nachvollziehbar verarbeitet werden. Nachfolgende Fehler verstoßen gegen diese Grundsätze der „*Rechtmäßigkeit, Fairness und Transparenz*“:

### 2.1. Rechtmäßigkeit

- 2.1.1. Es findet eine Verarbeitung statt, die nicht rechtmäßig ist (vgl. z.B. Kapitel A 4.5 ff.)

### 2.2. Verarbeitung nach Treu und Glauben

- 2.2.1. Das Cookie-Banner enthält zwar einen Link zur Datenschutzerklärung und dem Impressum bzw. verdeckt dieses nicht, klickt man auf die Links sind die Inhalte der Erklärungen jedoch durch das erneut angezeigte Banner verdeckt – es muss mithin eine Entscheidung getroffen werden, bevor man sich informieren kann.
- 2.2.2. Unzumutbare Kenntnisnahme, z.B. Nennung vieler hundert Empfänger.

- 2.2.3. Die Website speichert Einwilligungen (z.B. mittels Cookies), aber nicht die Verweigerung der Einwilligung oder die beschränkte Auswahl, und fragt deshalb permanent bei jedem Besuch erneut die Einwilligung ab. Hier ist zusätzlich die Gefahr gegeben, dass wiederkehrende Elemente plötzlich andere Inhalte haben, was dem Nutzer nach vielfachem An- oder Wegklicken aber nicht mehr auffallen muss. Beispiel: Ein Kreuz im Banner dient nur dazu, das Banner während des aktuellen Webseitenbesuches wegzuklicken, es wird aber keine Ablehnung gespeichert.
- 2.2.4. Es wird ein Button „alles akzeptieren“ angeboten, nicht jedoch auf derselben Ebene des Einwilligungs-Fensters ein Button „alles ablehnen“, der sowohl verweigerter Einwilligungen als auch erklärte Widersprüche (Artikel 21 DS-GVO) umfasst. Verweigerung und Widerspruch müssen so einfach sein wie die Erklärung der Einwilligung.
- 2.2.5. Ein Einwilligungsbanner ist so gestaltet, dass durchschnittlich verständige Nutzer davon ausgehen, dass sie alle Verarbeitungen und Cookies und ähnliche Techniken abgelehnt haben, in Wirklichkeit finden aber dennoch einwilligungsbedürftige Verarbeitungen oder das Speichern und Auslesen von Informationen auf dem Endgerät statt.
- 2.2.6. Ein Einwilligungsbanner zeigt zuerst nur einige Empfänger von Daten auf, erst beim Scrollen in der Liste werden weitere nachgeladen und die Nutzenden über die Länge der Liste getäuscht.
- 2.2.7. Ein Einwilligungsbanner zeigt zuerst nur einige Empfänger von Daten auf, beim Scrollen wird optisch ein Nachladen von weiteren Elementen suggeriert und eine Wartepause eingelegt, obwohl gar keine Daten nachgeladen werden.
- 2.2.8. Es finden heimliche, nicht unter der Kontrolle der betroffenen Person stehende Tracking-Maßnahmen wie Fingerprinting statt.
- 2.2.9. Impressum oder Datenschutzinformationen werden von einem Banner verdeckt oder sind nicht erreichbar.
- 2.2.10. Es erscheint ein Einwilligungs-Banner, aber durch Scrollen auf der Seite werden alle Cookies und Verarbeitungen akzeptiert.
- 2.2.11. Es wird zwar suggeriert, dass alle Verarbeitungen deaktiviert sind, in den Untermenüs finden sich aber weitere Einstellungen, die manuell deaktiviert werden müssen.
- 2.2.12. Der Inhalt (abseits von Überschrift und Einleitung) ist nur mit einem Bezahl-Abo erreichbar, bei Einholung der Einwilligung ist dies aber nicht erkennbar.

### 2.3. Transparenz

- 2.3.1. Es ist intransparent, welche Verarbeitungen auf welcher Rechtsgrundlage stattfinden, beispielsweise weil darüber nicht ausreichend informiert wird.
- 2.3.2. Es findet Nudging statt: Nutzende werden unterschwellig zur Abgabe einer Einwilligung beeinflusst. Das ist beispielsweise dann der Fall, wenn Buttons/Schaltflächen durch eine farbliche Hervorhebung, Größe oder Position deutlich auffälliger gestaltet sind.

### 3. Datenverarbeitung ohne Einwilligung

Grundsätzlich erlaubt die DS-GVO, Verarbeitungen personenbezogener Daten auf andere Rechtsgrundlagen als die Einwilligung zu stützen.

#### 3.1. Vertrag

Die Datenverarbeitung wird auf einen Vertrag (Artikel 6 Absatz 1 Buchstabe b DS-GVO) gestützt.

- 3.1.1. Es wird behauptet, Datenverarbeitungen sei funktionsnotwendig zur Erbringung der vom Nutzer nachgefragten bzw. vertraglich vereinbarten Dienste, ohne, dass sie dies wirklich sind, z.B. weil ...
  - 3.1.1.1. ... technisch nicht unbedingt erforderliche Cookies gesetzt oder ausgelesen werden,
  - 3.1.1.2. ... Verarbeitung von Artikel-9-Daten erfolgt, ohne dass die Voraussetzungen des Artikel 9 Absatz 2 DS-GVO vorliegen,
  - 3.1.1.3. ... Trackingdaten mit „Offline-Daten“ vermengt werden,
  - 3.1.1.4. ... Analysedienste mit Übermittlung genutzt werden,
  - 3.1.1.5. ... anbieterübergreifendes Tracking stattfindet,
  - 3.1.1.6. ... Übermittlung an Dritte durchgeführt wird.

#### 3.2. Berechtigtes Interesse

Die Verarbeitung wird auf ein „berechtigtes Interesse“ (Artikel 6 Absatz 1 Buchstabe f DS-GVO) gestützt, jedoch ...

- 3.2.1. ist die Datenverarbeitung einer Abwägung nach Artikel 6 Absatz 1 Buchstabe f DS-GVO schon im Ansatz nicht zugänglich, weil gemäß § 25 TTDSG das Ablegen/Auslesen von Informationen auf/von Endgeräten nur bei strenger Funktionsnotwendigkeit oder mit Einwilligung erlaubt ist.
- 3.2.2. werden, obschon eine Abwägung nach Artikel 6 Absatz 1 Buchstabe f DS-GVO zugunsten des Verantwortlichen ausgeht, Informationen auf den Endgeräten der Nutzenden abgelegt oder ausgelesen, so dass eine Einwilligung aufgrund § 26 TTDSG erforderlich ist.
- 3.2.3. ist der Verantwortliche eine öffentliche Stelle oder Behörde bei der Erfüllung ihrer Aufgaben und kann sich daher nicht auf Artikel 6 Absatz 1 Buchstabe f DSGVO berufen (vgl. Unterabsatz 2 DS-GVO).
- 3.2.4. wird nicht zugleich über das Widerspruchsrecht informiert (Artikel 21 Absatz 4 DS-GVO).
- 3.2.5. wird kein Widerspruchsrecht eingeräumt bzw. Widersprüche werden nicht oder nicht ausreichend/angemessen beachtet (Artikel 21 Absatz 3 bzw. Absatz 1 Satz 2 DS-GVO).
- 3.2.6. ist die vorgesehene Widerspruchsmöglichkeit nicht zumutbar.
- 3.2.7. wird die geplante Datenverarbeitung nicht hinreichend konkretisiert. Bsp.: Ein Verantwortlicher gibt an, aufgrund Artikel 6 Absatz 1 Buchstabe f DS-GVO Datenverarbeitungen durchzuführen zwecks Missbrauchs- und Betrugsprävention. Während dies „an sich“ ein

tauglicher Zweck sein mag, ist zur Erreichung dieses Zwecks aber nicht jedwede Datenverarbeitung erlaubt. Daher kann der pauschale Hinweis auf „Datenverarbeitungen“ nicht ausreichend sein.

- 3.2.8. wird der mittels erkennbarer Standard-Verfahren erklärte Widerspruch (z.B. Do not Track, o.ä.) nicht beachtet.
- 3.2.9. wird, obwohl die betroffene Person den privaten Browser-Modus nutzt, versucht, sie über verschiedene Sitzungen hinweg dauerhaft wiederzuerkennen, beispielsweise mittels Fingerprinting.
- 3.2.10. trägt eine Abwägung nicht die Verarbeitung, weil die Interessen des Betroffenen überwiegen, z.B. bei ...
  - 3.2.10.1. ... Einsatz von Analysediensten mit Übermittlung,
  - 3.2.10.2. ... Verknüpfung mit Offline-Daten,
  - 3.2.10.3. ... anbieterübergreifendem Tracking,
  - 3.2.10.4. ... Ausspielung personalisierter Anzeigen,
  - 3.2.10.5. ... Übermittlung an Dritte,
  - 3.2.10.6. ... Verarbeitungen, die der Produktentwicklung des Anbieters oder eines Dritten dienen,
  - 3.2.10.7. ... Verknüpfung der Daten aus verschiedenen Geräten,
  - 3.2.10.8. ... heimlichem und grundsätzlich schwer zu kontrollierendem Fingerprinting.

#### 4. Einhaltung der Betroffenenrechte

Um den Pflichten aus Kapitel 3 der DS-GVO gerecht zu werden, müssen Verantwortliche ausführlich über die Verarbeitungen informieren und zudem Betroffenen auf Antrag alle Informationen, die sie über die betroffenen Personen speichern, beauskunften. Je komplexer die Verarbeitungen sind, desto mehr Vorbereitungen sind nötig. Nachfolgende Fehler verstoßen gegen die „*Informationspflicht(en)*“:

- 4.1.1. Es sind keine Informationen nach Artikel 13 (und evtl. 14) DS-GVO vorhanden.
- 4.1.2. Die Information erfolgt nicht in präziser, transparenter, verständlicher und leicht zugänglicher Form, insbesondere sind die Informationen ...
  - 4.1.2.1. ... übermäßig lang,
  - 4.1.2.2. ... unübersichtlich,
  - 4.1.2.3. ... nicht in deutscher Sprache erhältlich ist, obwohl sich das Angebot an deutschsprachige Nutzer richtet.
- 4.1.3. Es sind nur unzureichende Informationen nach Artikel 13 oder 14 DS-GVO vorhanden, insbesondere ...
  - 4.1.3.1. ... fehlen Informationen zum Verantwortlichen,
  - 4.1.3.2. ... werden nicht alle Verarbeitungen genannt,
  - 4.1.3.3. ... wird keine klare und einfache Sprache verwendet
  - 4.1.3.4. ... wird nicht ausreichend über Zwecke und Rechtsgrundlagen informiert,
  - 4.1.3.5. ... wird nicht oder nicht ausreichend über Empfänger der Daten informiert,
  - 4.1.3.6. ... wird nicht oder nicht ausreichend über stattfindende Drittstaaten-Transfers informiert,
  - 4.1.3.7. ... fehlen Informationen zu den Betroffenenrechten oder sind unvollständig.

- 4.1.4. Eine Auskunft nach Artikel 15 DS-GVO wird nicht vollständig erteilt bzw. Verantwortliche haben keine Prozesse, um solche Auskünfte zu beantworten.
- 4.1.5. Verantwortliche verarbeiten zwar personenbezogene Daten anhand von eindeutigen Cookie-IDs (Pseudonymen), beantworten Anfragen nach Artikel 15 DS-GVO unter Nennung dieser IDs aber nicht oder nicht vollständig.
- 4.1.6. Obwohl die Verarbeitung auf eine Einwilligung oder einen Vertrag gestützt wird, haben Betroffene keine Möglichkeit, ihr Recht nach Datenübertragbarkeit (Artikel 20 DS-GVO) geltend zu machen.
- 4.1.7. Der Verantwortliche ist nicht in der Lage, Anträgen betroffener Personen auf Löschung (Artikel 17 DS-GVO), Berichtigung (Artikel 16 DS-GVO) oder Widerspruch (Artikel 21 DS-GVO) nachzukommen.

## 5. Drittstaatentransfer

Bei Übermittlungen personenbezogener Daten in Drittländer sind die Anforderungen aus Kapitel 5 der DS-GVO zu beachten. Typische Fehler im Rahmen eines „Drittstaatentransfers“ sind:

- 5.1.1. Es wird nicht deutlich, wie das grundsätzliche Verbot von Drittlandsübermittlungen gemäß Kapitel 5 der DS-GVO überwunden wird, insbesondere weil ...
  - 5.1.1.1. ... das „Privacy Shield“ unwirksam ist, sich der Verantwortliche aber noch darauf beruft,
  - 5.1.1.2. ... Standardvertragsklauseln nicht zu einem angemessenen Datenschutzniveau führen,
  - 5.1.1.3. ... massenweise Datenverarbeitungen in Drittstaaten nicht auf Einwilligungen gestützt werden können (Artikel 49 Absatz 1 Satz 1, Satz 2 DS-GVO).
- 5.1.2. Es werden keine ausreichenden zusätzlichen Maßnahmen („Supplementary Measures“) bei Drittstaatentransfer durchgeführt.

Weitere Informationen sind der Orientierungshilfe Schrems II<sup>21</sup> zu entnehmen.

## 6. Auftragsverarbeitung

Nachfolgende Punkte verstoßen gegen die Anforderungen an eine rechtskonforme Auftragsverarbeitung:

- 6.1.1. Es wurde kein Vertrag zur Auftragsverarbeitung geschlossen.
- 6.1.2. Der Vertrag zur Auftragsverarbeitung entspricht nicht den Anforderungen aus Artikel 28 DS-GVO, insbesondere ...
  - 6.1.2.1. ... ein Auftragsverarbeiter verarbeitet personenbezogene Daten auch zu eigenen Zwecken und sprengt so die Grenzen des Artikel 28 DS-GVO.
  - 6.1.2.2. ... ein Auftragsverarbeiter bestimmt die Zwecke und Mittel der Verarbeitung selbst.

---

<sup>21</sup> Orientierungshilfe: Was jetzt in Sachen internationaler Datentransfer?, siehe <https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2021/10/OH-int-Datentransfer.pdf>

## 7. Gemeinsame Verantwortung

Nachfolgende Punkte verstoßen gegen die Anforderungen der DS-GVO im Rahmen der gemeinsamen Verantwortlichkeit:

- 7.1.1. Es liegt eine gemeinsame Verantwortung im Sinne des Artikel 26 DS-GVO vor, aber ...
  - 7.1.1.1. eine entsprechende Vereinbarung wurde nicht geschlossen,
  - 7.1.1.2. entsprechende Informationen fehlen,
  - 7.1.1.3. die Vereinbarung hält die Bedingungen der DS-GVO nicht ein.

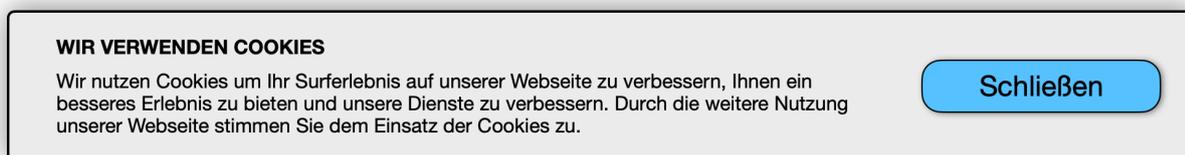
## Abschnitt C: Beispiele für Banner

Die folgenden Beispiele zeigen exemplarisch einige der in Abschnitt B dargestellten häufig auftretenden Fehler, die Verantwortliche bei der Einholung von Einwilligungen im Kontext von Cookies und Tracking machen.

Bei der Bewertung der Beispiele gehen wir davon aus, dass typische Cookies und einwilligungsbedürftige Verarbeitungen genutzt werden: Es werden Elemente von Drittanbietern wie Analyse-, Remarketing- und Werbe-Tools eingebunden, die mittels Verhaltensbeobachtung (z.B. Protokollierung aller aufgerufenen Webseiten) personenbezogenen Dossiers über die Nutzer\_innen erstellen, mit Offline-Daten verknüpfen und diese auch an beliebig viele Dritte weitergeben können. Die jeweils aufgeführte Bewertung ist exemplarisch und immer auch anhand der konkret stattfindenden Verarbeitungen zu messen; in der Praxis können sich im konkreten Einzelfall daher auch andere Bewertungen ergeben.

Viele Banner haben mehrere Ebenen und zeigen auf tieferen Ebenen weitere Informationen an. Zur besseren Übersicht beschränken sich die folgenden Beispiele auf die 1. Ebene. Grundsätzlich können auf weiteren Ebenen durchaus weitere Informationen gegeben werden. Auf der ersten Ebene sind aber alle relevanten Informationen darzustellen, damit Nutzende in der Lage sind, eine informierte Willensentscheidung zu treffen. Abschnitt A 4.7 ist besonders zu beachten.

### Beispiel 1



**WIR VERWENDEN COOKIES**

Wir nutzen Cookies um Ihr Surferlebnis auf unserer Webseite zu verbessern, Ihnen ein besseres Erlebnis zu bieten und unsere Dienste zu verbessern. Durch die weitere Nutzung unserer Webseite stimmen Sie dem Einsatz der Cookies zu.

Schließen

Als Verstöße kommen unter anderem in Betracht:

- Es ist keine Rechtsgrundlage für die Verarbeitung ersichtlich, eine Einwilligung wird nicht eingeholt (vgl. auch B 3)
- Es finden einwilligungsbedürftige Verarbeitungen bereits statt, ohne dass Nutzende überhaupt mit der Seite interagieren (B 1 und insbesondere 1.1.1)
- Unvollständige Information (B 1.3.5)
- Freiwilligkeit der Einwilligung fraglich (B 1.2)
- Es wird über das Ausmaß der Verarbeitung getäuscht (B 1.3.8.3), wenn die in der Einleitung zu Abschnitt B erwähnten Verarbeitungen tatsächlich vorgenommen werden
- Es wird keine aktive Einwilligung eingeholt (B 1.4)
- Die Informationspflichten werden nicht eingehalten (B 4).

## Beispiel 2

**Auch diese Seite verwendet Cookies!**

Diese Website verwendet Cookies. Cookies sind kleine Textdateien, die auf ihrem Computer abgelegt werden und uns helfen, unsere Website ideal zu gestalten. Für den optimalen Websitebesuch empfehlen wir, alle Cookies zu akzeptieren. Zum Verwalten oder Ausschalten von Cookies bitte auf „Cookie-Einstellungen“ klicken oder unsere [Cookie-Richtlinie lesen](#), um mehr Informationen zu erhalten.

[Alle Cookies akzeptieren](#)

[Cookie-Richtlinie](#)

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.74.5 )
- Es wird über das Ausmaß der Verarbeitung getäuscht (B 1.3.8.3), wenn die in der Einleitung zu Abschnitt B erwähnten Verarbeitungen tatsächlich vorgenommen werden
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information in einfacher Sprache (B 1.3.9)
- Information nur zu Cookies, nicht zu den Verarbeitungen (B 1.3.5.1)
- Ablehnen ist nicht möglich (oder nicht ersichtlich) (B 1.2.2)

## Beispiel 3

**Wir Respektieren Ihre Privatsphäre!**

---

Unsere Partner und wir verwenden nicht-sensible Daten wie Cookies oder Geräteidentifikatoren, um personalisierte Werbung anzuzeigen, Traffic und Besucherpräferenzen zu messen und Inhalte zu personalisieren.

Klicken Sie auf die Schaltfläche, um Ihr Einverständnis mit diesen Vorgängen auszudrücken und maßgeschneiderte Inhalte zu genießen. Sie können Ihre Präferenzen jederzeit ändern, indem Sie diese Website erneut besuchen.

[Mehr erfahren](#) [Annehmen](#)

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.7)
- Keine gleichwertige Möglichkeit der Ablehnung (B 2.2.4)
- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Nur Beschreibung des Ergebnisses, nicht der Verarbeitung selbst (B 1.3.8.2)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information in einfacher Sprache (B 1.3.9)
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)
- Falsche Aussagen über die Eingriffsintensität (B 0)
- Falsche Aussagen über die Sensibilität der Daten (B 1.3.8.6)

## Beispiel 4

### Ihre Privatsphäreinstellungen

Für die zuverlässige und komfortable Bereitstellung dieses Angebots werden auf dieser Seite technisch notwendige Cookies gesetzt. Zudem wird ein Cookie gesetzt, welches den aktuellen Status Ihrer Privatsphäreinstellung speichert (Auswahl-Cookie).

Mit der Ausnahme des Auswahl-Cookie werden technisch nicht notwendige Cookies zur Verbesserung des Benutzungserlebnisses (Comfort Cookies) und individualisierte Angebote (Marketing Cookies und Tracking-Mechanismen) nur eingesetzt, wenn Sie uns vorher hierzu Ihre Einwilligung gegeben haben:

**Komfort zustimmen**  
Mehr Informationen

**Marketing zustimmen**  
Mehr Informationen

Wenn Sie auf „Speichern“ klicken, werden ausschließlich die von Ihnen ausgewählten Cookies eingesetzt. Sie können Ihre hier erteilte Einwilligung jederzeit mit Wirkung für die Zukunft unter Privatsphäreinstellungen widerrufen.

**Alle Akzeptieren**

Speichern

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.7)
- Keine gleichwertige Möglichkeit der Ablehnung (B 2.2.4)

- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Nur Beschreibung des Ergebnisses, nicht der Verarbeitung selbst (B 1.3.8.2)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information in einfacher Sprache (B 1.3.9)W
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)
- Falsche Aussagen über die Eingriffsintensität (B 0)
- Falsche Aussagen über die Sensibilität der Daten (B 1.3.8.6)

## Beispiel 5

Wir glauben, dass Ihre Daten Ihr Eigentum sind und unterstützen Ihr Recht auf Privatsphäre und Transparenz.

Wählen Sie eine Datenzugriffsebene und -dauer aus, um auszuwählen, wie wir Ihre Daten verwenden und weitergeben.

SILBER  GOLD  PLATIN 3 Monate ▾

Höchste Privatsphäre. Datenzugriff nur für notwendige Website-Operationen. Die Daten werden an Dritte weitergegeben, um sicherzustellen, dass die Website sicher ist und auf Ihrem Gerät funktioniert

**Einstellungen Speichern**

Als Verstöße kommen unter anderem in Betracht:

- Irreführende Auswahlmöglichkeiten (B 1.3.12)
- Unverständliche Information (B 1.3.11)
- Missverständliche Überschrift (B 1.3.7)
- Inhaltlich falsche Information (B 1.3.8)
- Keine gleichwertige Möglichkeit der Ablehnung (B 2.2.4)
- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information in einfacher Sprache (B 1.3.9)
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)
- Information nur zu Cookies, nicht zu den Verarbeitungen (B 1.3.5.1)

## Beispiel 6

**Wir benötigen Ihre Einwilligung, um fortzufahren.**

Um unsere Webseite für Sie optimal gestalten und verbessern zu können, verwenden wir Cookies.

Weitere Informationen zu Cookies erhalten Sie in unserer [Datenschutzerklärung](#).

Technisch notwendige Cookies

Drittanbieter-Cookies (Social-Media-Elemente von Facebook, Twitter und Google werden auf der gesamten Webseite aktiviert.)

**Alle Akzeptieren** **Akzeptieren**

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.7)
- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Nur Beschreibung des Ergebnisses, nicht der Verarbeitung selbst (B 1.3.8.2)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information (B 1.3.9)
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)
- Irreführende Auswahlmöglichkeiten (B 1.3.12)
- Information nur zu Cookies, nicht zu den Verarbeitungen (B 1.3.5.1)

Sofern in einem solchen Beispiel tatsächlich nur technisch unbedingt erforderliche Cookies gesetzt werden (vgl. A 1.3 und OH Telemedien 2021) und bei der Einbindung von Social-Media-Elementen die Hinweise aus A 2 und insbesondere A 2.2 beachtet werden, wäre grundsätzlich gar kein pauschaler Einwilligungs-Banner auf jeder Seite nötig. Eine Einwilligung nach DS-GVO wäre die falsche Rechtsgrundlage, da sie suggeriert, dass Nutzende diese widerrufen könnten, obwohl das bei technischer Notwendigkeit nicht möglich ist.

## Beispiel 7

### Ihr Nutzungserlebnis auf unserer Webseite

Wenn Sie unsere Webseiten besuchen, kann Ihre Systemsoftware Informationen in Form von Cookies oder anderen Technologien von uns und unseren [Partnern](#) abrufen oder speichern, um z.B. die gewünschte Funktion der Website zu gewährleisten und Ihr Nutzungserlebnis zu steigern. Durch diese Informationen werden Sie nicht direkt identifiziert. Die Informationen (z.B. IP-Adresse) nutzen wir, um personalisierte Anzeigen und Inhalte anzuzeigen sowie Anzeigen- und Inhaltsmessungen vorzunehmen und Erkenntnisse über Zielgruppen und Produktentwicklungen zu gewinnen. Mit Ihrem Recht auf selbst bestimmten Datenschutz, können Sie sich entscheiden, bestimmte Arten von Cookies nicht zuzulassen, soweit es sich nicht um (technisch) unbedingt erforderliche Cookies handelt. Wenn Sie den Button „Alles akzeptieren“ anklicken, stimmen Sie zu, dass Ihre Informationen [wie beschrieben](#) verwendet werden. Über den Button „Einstellungen“ können Sie mehr über die eingesetzten Cookies erfahren und Ihre Wunscheinstellungen vornehmen. Die Blockierung bestimmter Arten von Cookies kann jedoch zu einer beeinträchtigten Erfahrung unserer Websites und Dienste führen.

Verschiedene Cookies werden von Partnern ggf. auch mit Sitz in den USA gesetzt. Hierzu zählen Trackingtools, wie z.B. Google Analytics. Diese sind standardmäßig deaktiviert. Durch die Einwilligung stimmen Sie zugleich einer Übermittlung Ihrer Daten in die USA zu ([Einwilligung internationaler Datentransfer](#)). Bitte beachten Sie, dass der US Dienstleister womöglich kein Datenschutzniveau bereithält, das dem Schutzniveau in EU/EWR/Schweiz entspricht.

Einstellungen

Alle Akzeptieren

[Impressum](#) | [Datenschutzhinweise](#)

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.7)
- Keine gleichwertige Möglichkeit der Ablehnung (B 2.2.4)
- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Nur Beschreibung des Ergebnisses, nicht der Verarbeitung selbst (B 1.3.8.2)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Unzumutbare optische Gestaltung (B 1.3.3.1)
- Drittstaatentransfer (B 5), insbesondere massenweise Datenverarbeitung in Drittstaaten aufgrund Einwilligung (B 5.1.1.3)
- Es wird teilweise nur über Cookies, nicht aber über die Verarbeitungen informiert (B 1.3.5.1)
- Es findet Nudging statt (B 2.3.2)
- Keine präzise Information in einfacher Sprache (B 1.3.9)
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)

Grundsätzlich ist denkbar, weitere Informationen auf einer 2. Ebene darzustellen. Auf der 1. Ebene sind aber dennoch ausreichende Informationen über die Verarbeitungen und deren Ausmaß zu geben, damit Nutzende eine in informierter Weise freie Willensentscheidung treffen können.

## Beispiel 8

### Herzlich Willkommen!

#### Weiter mit Werbung

Besuchen Sie den frei verfügbaren Teil unserer Webseite wie gewohnt mit Werbung, üblichem Tracking und Cookies. Details finden Sie in den [Datenschutzhinweisen](#). Ihre Zustimmung ist jederzeit widerrufbar!

**Akzeptieren & schließen**

#### ... oder Pur-Abo ohne Cookies\*

Nutzen Sie den frei verfügbaren Teil unserer Webseite ganz ohne personalisierte Werbung, ohne dem üblichem Tracking und ohne Cookies\* für nur 4,99 EUR/Monat.

**Informationen zum Abo**

Tracking: Um unser Angebot optimal gestalten zu können sowie zur Verbesserung und Finanzierung unseres Angebots arbeiten wir mit bis zu 256 Partnern und Drittanbietern zusammen. Diese Drittanbieter und wir erheben und verarbeiten personenbezogene Daten auf unseren oder ihren eigenen Plattformen. Mit auf Ihrem Gerät gespeicherten Cookies und anderen Technologien oder von uns oder unseren Partnern auf Ihrem Gerät gespeicherten Informationen, persönlichen Identifikatoren wie bspw. Geräte-Kennungen oder IP-Adressen sowie basierend auf Ihrem individuellen Nutzungsverhalten, Ihrem offline-Einkaufsverhalten und weiteren Daten können wir und diese Drittanbieter Personalisierte Anzeigen und Inhalte, Anzeigen- und Inhaltsmessungen, Erkenntnisse über Zielgruppen und Produktentwicklungen ausspielen. Es können mehr Daten hinzugefügt werden, um Anzeigen und Inhalte besser zu personalisieren.

Durch das Klicken des „Akzeptieren“-Buttons stimmen Sie der Verarbeitung der auf Ihrem Gerät bzw. Ihrer Endeinrichtung gespeicherten Daten wie z.B. persönlichen Identifikatoren oder IP-Adressen für die notwendigen Verarbeitungszwecke gem. § 25 Abs. 1 TTDSG sowie Art. 6 Abs. 1 lit. a DSGVO zu. Darüber hinaus willigen Sie gem. Art. 49 Abs. 1 DSGVO ein, dass auch Anbieter in den USA Ihre Daten verarbeiten. Die USA werden vom Europäischen Gerichtshof als ein Land mit einem nach EU-Standards unzureichendem Datenschutzniveau eingeschätzt. Es besteht insbesondere das Risiko, dass Ihre Daten durch US-Behörden, zu Kontroll- und zu Überwachungszwecken, möglicherweise auch ohne Rechtsbehelfsmöglichkeiten, verarbeitet werden können. Weiterführende Details finden Sie in unserer Datenschutzhinweisen, die am Ende jeder Seite verlinkt sind. Dort können Sie Ihre Zustimmung jederzeit widerrufen.

\* Im Pur-Abo werden keine einwilligungspflichtigen Datenverarbeitungen vorgenommen und nur solche Cookies und ähnliche Technologien verwendet, die zur Erbringung dieses Dienstes unbedingt erforderlich sind.

[Impressum](#) | [Datenschutzhinweise](#) | [Nutzungsbedingungen](#)

Als Verstöße kommen unter anderem in Betracht:

- Missverständliche Überschrift (B 1.3.7)
- Unzumutbare optische Gestaltung (B1.3.3.1)
- Täuschung über den wahren Zweck der Datenverarbeitung (B 1.3.8.1)
- Nur Beschreibung des Ergebnisses, nicht der Verarbeitung selbst (B 1.3.8.2)
- Täuschung über Ausmaß der Verarbeitung (B 1.3.8.3)
- Drittstaatentransfer (B 5), insbesondere massenweise Datenverarbeitung in Drittstaaten aufgrund Einwilligung (B 5.1.1.3)
- Keine präzise Information in einfacher Sprache (B 1.3.9)
- Keine ausreichende Information über die Verarbeitungen (B 1.3.5.4)

Es stellt sich zudem die Frage, ob alle Verarbeitungen tatsächlich erforderlich sind (Datenminimierung, Artikel 5 Absatz 1 Buchstabe c DS-GVO)