Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

FAQ zu Cookies und Tracking

durch Betreiber von Webseiten und
Hersteller von Smartphone-Apps

Version 1.0.1 vom 29. April 2019

Betreiber von Webseiten, aber auch Hersteller von Smartphone-Apps (sog. „Anbieter von Telemediendiensten“) müssen sicherstellen, dass bei der Verarbeitung personenbezogener Daten alle Vorgaben der Datenschutz-Grundverordnung (DSGVO) eingehalten werden. Die bisherigen Datenschutz-Regelungen des Telemediengesetzes (TMG) können seit Mai 2018 insbesondere auf die Einbindung von Elementen Dritter und webseitenübergreifendes Tracking nicht mehr angewendet werden, wie in der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien[1] (im Folgenden: Orientierungshilfe) dargestellt.

Die folgende Beschreibung bezieht sich im Wesentlichen auf Websites, gilt sinngemäß aber auch für Apps auf Smartphones und Tablets oder Desktop-Programmen. Die folgenden FAQ geben einen Überblick zu Cookies und Tracking, nähere Informationen finden sich in der genannten Orientierungshilfe.

1. Darf ich Werkzeuge zur Reichweitenanalyse ohne Einwilligung der Nutzer verwenden?

Ja, wenn für die Reichweitenanalyse nicht auf die Dienste externer Dritter zurückgegriffen wird. Eine Reichweitenanalyse funktioniert nämlich auch ohne Dritten (wie Google Analytics) Informationen über das Nutzungsverhalten der Website-Besucher weiterzugeben. Stattdessen kann eine **Logfile-Analyse** gemacht oder es können **lokal installierte Analysewerkzeuge**[2] ohne Zusammenführung der Nutzungsdaten über Anbietergrenzen hinweg verwendet werden (siehe Kasten auf Seite 13 der Orientierungshilfe). Auch diese müssen transparent dargestellt (vgl. Art. 12 ff. DSGVO) und datensparsam konfiguriert werden. Verantwortliche Seitenbetreiber ersparen sich damit den Aufwand für eine datenschutzrechtliche Untersuchung externer Dienste im Einzelfall und das Einholen der ausdrücklichen Einwilligung der Nutzer (siehe Frage 5 dieser FAQ sowie Seite 8 ff der Orientierungshilfe).

Bei der Einbindung von **Elementen Dritter,** z.B. Reichweiteanalyse-Tools oder Social-Media-Plugins, ist regelmäßig eine Einwilligung in die konkrete Datenverarbeitung erforderlich (vgl. Anhang I der

[1] Online verfügbar unter https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/Orientierungshilfe-der-Aufsichtsbehörden-für-Anbieter-von-Telemedien.pdf.

[2] Ein Beispiel für ein entsprechendes Analyse-Tool ist die kostenlose Open-Source-Software Matomo, siehe https://matomo.org/ – aber auch hier sind datenschutzfreundliche Voreinstellungen zu wählen.

Orientierungshilfe). Eine **ausdrückliche, informierte, freiwillige, aktive und vorherige Einwilligung** der Nutzer 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 Elemente wie Social-Media-Plugins oder 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.

2. Welche Cookies darf ich ohne Einwilligung nutzen?

Bei der Verwendung von Cookies, die zum Betrieb des Telemediendienstes notwendig sind und keine seitenübergreifende Nachverfolgung des Nutzerverhaltens ermöglichen, können sich Verantwortliche häufig auf (vor-) **vertragliche Maßnahmen** Artikel 6 Absatz 1 lit. b DSGVO 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.

In anderen Fällen können sich Verantwortliche auf ein **berechtigtes Interesse** nach Artikel 6 Absatz 1 lit. f DSGVO berufen. Wenn die entgegenstehenden Belange der Nutzer in diesen Fällen nicht überwiegen, ist die Nutzung von Cookies **nicht einwilligungsbedürftig**.

Weitere Informationen zu der durchzuführenden Interessenabwägung finden sich in der Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien.[3] Zum Widerspruchsrecht nach Artikel 21 DSGVO und entsprechende Voreinstellungen des Nutzers wie beispielsweise eine „Do Not Track" Einstellung siehe Seite 17 f der Orientierungshilfe.

3. Für welche Cookies und Tracking-Mechanismen brauche ich die Einwilligung der Nutzer?

Anbieter von Telemediendiensten, die Elemente integrieren, die das Nutzerverhalten insbesondere über Website- oder Geräte-Grenzen hinweg (also z.B. über verschiede Domains verschiedener Anbieter) zusammenfassen, benötigen die aktive, ausdrückliche, informierte, freiwillige und vorherige Einwilligung (Artikel 6 Absatz 1 lit. a DSGVO) der Nutzer (vgl. Seite 8 ff der Orientierungshilfe und Frage 5 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 ohne Einwilligung zusammenführen.

4. Darf ich Elemente Dritter wie Like und Share Buttons in meine Website einbinden?

Bei der Nutzung von Diensten Dritter (z. B. Analysetools oder Social Plugins) kommt es häufig zu Datenübermittlungen an Dritte. Eine solche Einbindung bedarf einer Rechtsgrundlage nach Artikel 6 Absatz 1 DSGVO. Mit **wenig Aufwand nutzbar** sind **datenschutzfreundliche Implementierungen** von

[3] Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf.

Like- und Share-Buttons[4], wenn sichergestellt ist, dass Informationen über das Nutzerverhalten ohne Einwilligung des Nutzers nicht an Dritte weitergegeben und nicht websiteübergreifend zusammengeführt werden. Social-Media-Elemente sollten über eine Zwei-Klick-Lösung oder mit Hilfe datenschutzfreundlicher Einbett-Hilfen[5] eingebunden werden. Bei einem Tracking über Website- oder Geräte-Grenzen hinweg ist die Einwilligung der Nutzer immer erforderlich (siehe Frage 3).

Hinweis: Die vorgelagerte Frage der Zulässigkeit des Betriebs von Social-Media-Accounts muss für jeden Dienst im Einzelfall separat geprüft werden.[6]

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

In der Einwilligung (vgl. Seite 8 ff der Orientierungshilfe) muss der Verarbeitungsvorgang **klar und deutlich** beschrieben werden. Nutzer müssen ohne weiteres verstehen können, in was 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 für die Verwendung von Cookies an sich, sondern für die Erhebung und Weitergabe personenbezogener Daten eingeholt werden. Insbesondere muss genau und verständlich aufgelistet werden, an welche **namentlich zu benennenden Dritten** welche Daten weitergegeben werden, bzw. welche Dritten Daten erheben oder empfangen (Empfänger) und zu welchem genauen Zweck dies geschieht. **Verfolgen Dritte eigene Zwecke,** müssen auch diese beschrieben werden. Diese Informationen müssen klar und deutlich dargestellt werden und dürfen nicht verschleiert werden, auch nicht durch die Wahl der Überschrift. Nutzer müssen **aktiv** und freiwillig einwilligen (Opt-In, siehe Kasten auf Seite 5 der Orientierungshilfe), die **Zustimmung darf nicht vorausgewählt** sein. Opt-Out-Verfahren oder bereits im Vorhinein angekreuzte Kästchen reichen nicht aus („privacy by design“ und „privacy by default“). Die einzelnen Empfänger sollten einzeln, bzw. nach Kategorien auswählbar sein. Vor einer aktiven Einwilligung des Nutzers dürfen **keine Daten** erhoben bzw. entsprechende Elemente nachgeladen werden. Auch das bloße Nutzen einer Website oder einer App stellt keine rechtmäßige Einwilligung dar.

Freiwillig ist die Einwilligung nur, wenn die betroffene Person eine **echte oder freie Wahl** (vergleiche Seite 10 der Orientierungshilfe) hat und eine Einwilligung auch verweigern kann, ohne dadurch 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.

---

[4] Wie z.B. mit Hilfe des c't-Projekts Shariff, siehe https://www.heise.de/ct/artikel/Shariff-Social-Media-Buttons-mit-Datenschutz-2467514.html , kostenlos als Open-Source-Software erhältlich unter https://github.com/heiseonline/shariff.

[5] Siehe z.B. das c’t-Projekt Embetty, https://www.heise.de/newsticker/meldung/Embetty-Social-Media-Inhalte-datenschutzgerecht-einbinden-4060362.html , kostenlos erhältlich als Open-Source-Software unter https://github.com/heiseonline/embetty.

[6] Zum Betrieb von Facebook Fanpages siehe https://www.datenschutzkonferenz-online.de/media/dskb/20190405_positionierung_facebook_fanpages.pdf.

6. Wie gestalte ich Einwilligungs-Banner?

Die Nutzung von Cookies ist nicht per se einwilligungsbedürftig. Datenverarbeitungen (ob mit oder ohne Hilfe von Cookies), für die keine Einwilligung erforderlich ist, müssen nur in der **Datenschutzerklärung** dargestellt werden. „Einwilligungs-Banner" müssen eingesetzt werden, wenn tatsächlich eine Einwilligung des Nutzers nötig ist, also insbesondere Daten an Dritte weitergegeben werden oder Dritten die Möglichkeit eröffnet wird, Daten zu erheben. In einem solchen Fall ist ein Hinweis auf Cookies in der Datenschutzerklärung nicht ausreichend, sondern es müssen die **oben genannten Anforderungen (siehe Frage 5)** und die **folgenden Vorgaben** für die Einwilligung beachtet werden (vergleiche Seite 8 ff der Orientierungshilfe):

Notwendige Elemente:

- 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"*. **Links** müssen **eindeutig** und unmissverständlich beschrieben sein – wesentliche Elemente/Inhalte insbesondere einer Datenschutzerklärung dürfen nicht durch Links verschleiert werden.
- 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?
- Die Einwilligung darf nicht voreingestellt sein – ein **Opt-in** ist notwendig (vgl. Seite 5 der Orientierungshilfe).
- Es dürfen **keine Daten weitergegeben** werden, **bevor eine Einwilligung** durch den Nutzer erteilt wurde.
- Der **Zugriff auf Impressum und Datenschutzerklärung** darf nicht verhindert oder eingeschränkt werden, bevor eine Einwilligung durch den Nutzer erteilt wurde.
- Die **Freiwilligkeit** der Einwilligungs-Erklärung muss deutlich gemacht werden und ein Hinweis auf das Recht auf einen **jederzeitigen Widerruf** muss enthalten sein; beispielsweise *„Diese Einwilligung ist freiwillig, für die Nutzung dieser Website nicht notwendig und kann jederzeit widerrufen werden, indem […]".*
- 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.