Sebastian Schwäbe

Technische Umsetzung beim Webtracking

Technische Anforderungen nach Einführung der Datenschutz-Grundverordnung

Seit Einführung der Datenschutz-Grundverordnung (DS-GVO) haben sich die Anforderungen an die Gestaltung von Webseiten verändert. Dieser Beitrag gibt einen Überblick der rechtlichen Rahmenbedingungen und stellt die technischen Umsetzungsmöglichkeiten näher dar.

1 Einführung

Nicht erst mit Inkrafttreten der Datenschutz-Grundverordnung (DS-GVO) finden sich auf fast jeder Webseite sogenannte Cookie-Banner, wenngleich die Zahl der Banner seit Einführung der Datenschutz-Grundverordnung noch erheblich zugenommen hat. Diese Banner werden als Ebene vor die eigentliche Webseite gelegt. Die Interaktion mit dem Banner soll in der Regel vom Nutzer eine Einwilligung für die Verarbeitungen seiner Daten einholen. Diese Banner werden Cookie-Banner genannt, weil es hier regelmäßig um die Platzierung von kleinen Textschnipseln, sogenannte Cookies, im Browser des Webseitenbesuchers geht. Cookies können unter anderem dazu genutzt werden, um in Kombination mit einem Tracking-Script Besucher auf der Seite zu verfolgen.

2 Warum eigentlich Cookies?

Webseiten werden auf sogenannten Webservern abgelegt und von diesen bereitgestellt. Die Kommunikation mit Webservern läuft über das Protokoll http(s) (Hyper Text Transport Protocol (Secure)). Diesem Protokoll ist zu eigen, dass es zustandslos ist. Jeder Aufruf einer Seite ist unabhängig von dem vorherigen oder dem nachfolgenden Aufruf und stellt eine eigene abgeschlossene Transaktion dar. Damit der Betreiber einer Webseite die jeweilige Sitzung des Benutzers aufrechterhalten kann, werden Cookies auf dem Gerät des Nutzers platziert. Diese Cookies werden fortan bei jedem Seitenaufruf an den Server des Webseitenbetreibers mitgeschickt. Der Server des Seitenbetreibers kann dadurch einen Zusammenhang zwischen einzelnen Transaktionen herstellen.

Sebastian Schwäbe

Rechtsanwalt und Berater bei der FIRST PRIVACY GmbH für internationalen Datenschutz und Informationssicherheit

E-Mail: sschwaebe@first-privacy.com

3 Verschiedene Formen von Cookies

Ganz grundsätzlich kann zwischen Session Cookies und permanenten Cookies unterschieden werden. Session Cookies werden vom Browser wieder gelöscht, sobald der Nutzer seine Sitzung, die sogenannten Session, beendet hat. Sie werden unter anderem genutzt, damit Nutzer auf einer Seite wiedererkannt werden können, während sie sich auf ihr bewegen. Permanente Cookies bleiben hingegen über eine Sitzung hinweg bestehen. Der Betreiber der Seite legt hierbei fest, wie lange die Cookies gültig sein sollen.

Ein Anwendungsfall für ein Session-Cookie wäre zum Beispiel ein Live-Chat für Kunden auf einer Webseite. Da der Chat in der Regel nur während der Session verwendet wird, kann das Cookie mit Ende der Sitzung wieder gelöscht werden. Würde hier kein Cookie gesetzt werden, um den jeweiligen Nutzer zu identifizieren, könnte nicht ohne weiteres zwischen einzelnen Chat-Teilnehmern unterschieden werden.

Ein permanentes Cookie wird immer dann verwendet, wenn Nutzer nicht nur in einer Session wiedererkannt werden sollen, sondern auch Session-übergreifend – also zum Beispiel beim nächsten Besuch der Webseite. Klassischer Anwendungsfall ist hier, dass ein Dienst die vorherige Anmeldung eines Nutzers erkennt. Manche Dienste bieten hierfür beim Anmelden eine Checkbox mit einem Titel wie „Angemeldet bleiben“ an.

Naturgemäß eignen sich sowohl Session- als auch Permanent-Cookies nicht nur dafür, um für den Nutzer das Nutzungserlebnis zu optimieren. Es lassen sich mit diesen Cookies auch Nutzer verfolgen, sodass der Webseitenbetreiber feststellen kann, welcher Nutzer welche Seite aufgerufen hat, indem ihm ein eindeutiges Cookie zugewiesen wird. Für dieses sogenannte Webtracking

gibt es eine Vielzahl von Diensten, wobei Google Analytics (mit dem wohl größten Marktanteil) oder Matomo (vormals Piwik) zu den bekanntesten Vertretern zählen dürften. Beide Dienste setzen in JavaScript geschriebene Tracking-Werkzeuge ein, die in den Browsern der jeweiligen Webseitenbesucher ausgeführt werden. Mit diesem JavaScript-Code lässt sich in Kombination mit Cookies beispielsweise feststellen, welche Seiten der Nutzer besucht hat, ob er eine Seite als Favorit abgelegt hat, ob er ein Konto auf der Seite erstellt hat, von welcher Seite er kommt, etc. Es lässt sich somit nachverfolgen, wie verschiedene Nutzer sich auf der Seite bewegen.

4 Die rechtliche Einordnung von Cookies und Tracking

Aus den obigen Ausführungen ergibt sich zwangsläufig, dass es nicht eine einzige Rechtsgrundlage für alle Cookies geben kann. Vielmehr ist der Zweck des jeweiligen Cookies, bzw. des damit in Zusammenhang stehenden Werkzeugs, zu beurteilen und die Frage zu klären, welche Daten verarbeitet werden. Maßgeblich für die Beurteilung der Rechtmäßigkeit ist hierfür die Datenschutz-Grundverordnung. Zwar sollte die Datenschutz-Grundverordnung ursprünglich durch die ePrivacy-Verordnung ergänzt werden (der „Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG“), da aber mit einer Verabschiedung der Verordnung in der nahen Zukunft nicht zu rechnen ist, muss die rechtliche Beurteilung nach der Datenschutz-Grundverordnung und den bis heute geltenden Gesetzen erfolgen.

Zu berücksichtigen ist, dass die ePrivacy-Verordnung die Nachfolge der Richtlinie 2002/58/EG (die sogenannte ePrivacy Richtlinie) antreten und diese außer Kraft setzen sollte, weshalb sich gut vertreten lässt, dass die aus der Richtlinie 2002/EG/EG folgenden Vorschriften nach wie vor Geltung entfalten.[1] Demnach spricht viel dafür, dass § 15 Abs. 3 TMG (der nach Ansicht der Bundesregierung[2] und der EU-Kommission[3] eine Umsetzung des 2002/58/EG darstellt) mangels Außerkrafttretens der ePrivacy Richtlinie nach wie vor spezialgesetzliche Rechtsgrundlage für die Datenverarbeitung ist. Und selbst, wenn davon ausgegangen wird, dass § 15 Abs. 3 TMG außer Kraft getreten ist, ließe sich Art. 6 Abs. 1 lit. f DS-GVO entsprechend auslegen, um das gleiche Ergebnis wie mit § 15 Abs. 3 TMG zu erzielen.

Doch auch wenn sich dieser Standpunkt sehr gut vertreten lässt, entschieden sich die Aufsichtsbehörden in einer gemeinsamen Stellungnahme vom 26.4.2018 dazu, § 15 Abs. 3 TMG für unanwendbar zu erklären.[4] Der bisherigen Rechtslage, wonach das Tracking auch ohne Einwilligung möglich war, wurde somit praktisch die Grundlage entzogen. Statt eines „Opt-Out“, wonach die Daten bis zum Widerspruch verarbeitet werden dürfen, ist nun grundsätzlich ein „Opt-In“ nötig. Eine Verarbeitung darf also erst dann stattfinden, wenn der Nutzer seine Einwilligung erklärt hat.

In der Positionsbestimmung findet sich hierzu in Ziffer 9 folgendes:

„Es bedarf jedenfalls einer vorherigen Einwilligung beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen. Das bedeutet, dass eine informierte Einwilligung i. S. d. Datenschutz-Grundverordnung, in Form einer Erklärung oder sonstigen eindeutig bestätigenden Handlung vor der Datenverarbeitung eingeholt werden muss, d. h. z. B. bevor Cookies platziert werden bzw. auf dem Endgerät des Nutzers gespeicherte Informationen gesammelt werden.“

Die Veröffentlichung der Positionsbestimmung einen Monat vor dem Inkrafttreten der Datenschutz-Grundverordnung

1 Vgl. auch *Venzke-Caprarese*, DuD2018, S. 156.

2 vgl. hierzu Plenarprotokoll 17/155 des Deutschen Bundestags, S. 18700 bis 18706, abrufbar unter https://dipbt.bundestag.de/dip21/btp/17/17155.pdf, zuletzt abgerufen am 16.06.2019.

3 BVDW Newsflash vom 11.02.2014, EU-Kommission bestätigt: E-Privacy-Richtlinie in Deutschland durch Telemediengesetz umgesetzt, abrufbar unter https://www.bvdw.org/presseserver/bvdw_eprivacy_tmg_20140211/nf_ePrivacy_Richtlinie_TMG_140211.pdf und Telemedicus, EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt, abrufbar unter https://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html, beide zuletzt abgerufen am 16.06.2019.

4 Zur Anwendbarkeit des TMG für nicht-öffentliche Stellen ab dem 25. Mai 2018, https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/Zur-Anwendbarkeit-des-TMG-fuer-nicht-oeffentliche-Stellen-ab-dem-25_-Mai-2018/Positionsbestimmung-TMG.pdf, zuletzt abgerufen am 16.6.2019.

führte nicht unbedingt zur Entspannung der Situation und stieß auf breiten Widerstand, sowohl auf Seiten von Seitenbetreibern als auch auf Seiten von Datenschützern.[5] Als Reaktion auf diese Positionsbestimmung nahmen Cookie-Banner in jedweder Form weiter zu, die um die Einwilligung des Nutzers buhlten. Ob hiermit tatsächlich dem Datenschutz gedient ist, darf bezweifelt werden: Da zuvor ein (einwilligungsfreies) Tracking der Nutzer zulässig war, wenn sich der Betreiber bei der Datenerhebung zurückhielt, hindert ihn nun nichts mehr daran, im Rahmen der Einwilligung ein Maximum an Trackingtechniken aufzufahren, für das er sich die Einwilligung des Besuchers zuvor eingeholt hat. Hinzu kommt, dass ein überwältigender Teil der Nutzer offenbar „schlicht genervt" von Cookie-Bannern ist und ohne Lektüre des Textes auf „Akzeptieren" oder „Ja" klickt. Ein Betreiber einer „Consent Management Platform" hat hier einmal ausgewertet, dass in der Regel über 90 % der Seitenbesucher ihre Einwilligung erklären.[6] Man kann an dieser Stelle wohl davon ausgehen, dass nur ein verschwindend geringer Teil der Nutzer sich die Mühe macht, die zugehörige Datenschutzerklärung zu lesen, um sich vor Abgabe seiner Einwilligung zu informieren. Der Umstand, dass die Cookie-Banner oft weite Teile oder gar die ganze Seite bedecken und Besucher in erster Linie Interesse an dem Inhalt haben, trägt sicherlich dazu bei, dass Nutzer dazu neigen, schnell eine Einwilligung abzugeben. Um von Cookie-Bannern verschont zu bleiben, haben sich bereits mehr als 110.000 Firefox Nutzer und über 214.000[7] Chrome Nutzer mit der Erweiterung „I don't care about cookies" versorgt, die jegliches Cookie-Banner verhindern.

Es bestehen also berechtigte Zweifel daran, dass der Weg über sogenannte Cookie-Banner zur Einholung einer Einwilligung der richtige ist. Es stellt sich zwangsläufig die Frage, ob er nicht vielmehr dazu führt, dass Datenschutz als ein Störfaktor und nicht als ein wichtiges Grundrecht wahrgenommen wird.

Ein Jahr nach der Unruhe durch die Positionsbestimmung hat sich die Datenschutzkonferenz dazu entschlossen, eine Orientierungshilfe für die Anbieter von Telemedien zu veröffentlichen, um Webseitenbetreibern eine Hilfestellung an die Hand zu geben.[8] Hier wird zwar nach wie vor an dem Standpunkt festgehalten, dass für die Anwendung von § 15 Abs. 3 TMG kein Raum bleibe, allerdings wird zumindest nicht ausgeschlossen, dass auch Art. 6 Abs. 1 S. 1 lit. f DS-GVO als Rechtsgrundlage für die Verarbeitung der Daten von Webseitenbesuchern in Frage kommen kann.

5 Rechtsgrundlagen der DS-GVO bei der Verarbeitung

Inwieweit ein Cookie-Banner überhaupt notwendig ist, richtet sich vor allem danach, ob die „Schwelle der Interessenabwägung" nach Art. 6 Abs. 1 lit. f DS-GVO überschritten ist und die Verarbeitung derart stark in die Rechte des Betroffenen eingreift, dass eine solche Verarbeitung nur über eine Einwilligung zu rechtfertigen ist.

Hieraus ergibt sich, dass viele Cookies keines Cookie-Banners bedürfen, weil die Verarbeitung auf Grundlage von Art. 6 Abs. 1 S. 1 lit. f DS-GVO zulässig ist. Da das deutsche Recht zum jetzigen Zeitpunkt keine Pflicht kennt, per Banner über den Einsatz von Cookies zu informieren, ist immer dann, wenn keine Einwilligung erforderlich ist, auch kein Cookie-Banner notwendig. Beispiele für derartige ohne Einwilligung mögliche Cookies können zum Beispiel (Session-)Cookies sein, die nur dem Zweck dienen, die Nutzerführung auf der Seite zu realisieren. Auch Cookies im Onlineshop für den Warenkorb fallen regelmäßig hierunter und benötigen keine Einwilligung, was auch die Aufsichtsbehörden in ihrer Orientierungshilfe entsprechend einschätzen.[9] Darüber hinaus ließe sich diskutieren, ob Warenkorbcookies nicht ebenfalls über Art. 6 Abs. 1 S. 1 lit. b DS-GVO zulässig sind, weil eine Bestellung im Webshop andernfalls überhaupt nicht möglich wäre. Da diese Cookies gesetzt werden müssen, um den Vertrag anzubahnen bzw. zu schließen kann man in diesen Fällen als Rechtsgrundlage Art. 6 Abs. 1 lit. b DS-GVO heranziehen. Und schließlich sehen die Aufsichtsbehörden auch Raum für die „Reichweitenmessung und statistische Analysen" auf Basis von Art. 6 Abs. 1 S. 1 lit. f DS-GVO.[10]

6 Verarbeitung mit Art. 6 Abs. 1 S. 1 lit. f DS-GVO

Wird Webtracking als ein (reines) Werkzeug zur Reichweitenmessung eingesetzt und entsprechend zurückhaltend konfiguriert, ist selbst ein Einsatz von Google Analytics oder Matomo über Art. 6 Abs. 1 S. 1 lit. f DS-GVO nicht ausgeschlossen.

Jedoch ist im Rahmen der Verarbeitung über die Interessenabwägung stets zu berücksichtigen, dass ein berechtigtes Interesse des Verantwortlichen oder eines Dritten vorliegen muss, die Datenverarbeitung zur Wahrung dieser Interessen erforderlich ist und die Interessen des Betroffenen – hier des Webseitenbesuchers – nicht die Interessen des Webseitenbetreibers überwiegen. Darüber hinaus muss wegen Art. 21 Abs. 1 DS-GVO dem Betroffenen ein Widerspruchsrecht eingeräumt werden. Unter Berücksichtigung dessen, hat der Betreiber der Seite ein durchaus berechtigtes Interesse daran, seine Webseite optimal zu gestalten, um sie möglichst interessant für die Besucher anzubieten. Um das zu ermöglichen, ist es erforderlich, dass der Betreiber auswertet, welche Nutzer in welchem Zeitraum welche Teile seiner Seite besuchen. Ebenso ist es von berechtigtem Interesse für den Betreiber, welche Spracheinstellung die Browser seiner Besucher haben und ob sie eher mit mobilen Geräten als mit stationären Geräten die Seiten besuchen.

Am Beispiel von Google Analytics könnte daher eine datenschutzkonforme Konfiguration wie folgt aussehen:

Die IP-Anonymisierung von Google Analytics wird eingesetzt, sodass das letzte Oktett der IPv4-Adresse des Besuchers bei der Besuchermessung nicht mehr verarbeitet wird. Dem Nutzer wird

5 https://www.datenschutz-notizen.de/google-analytics-und-matomo-ab-25-mai-2018-nur-noch-mit-einwilligung-4320396/ oder https://www.datenschutz-guru.de/aufsichtsbehorden-als-wegbereiter-fur-abmahner-von-internetseiten/, zuletzt abgerufen am 16.6.2019.

6 Vergleiche unter https://info.teads.tv/hubfs/+EMEA+/2018%2011_GDPR_Barometer_One-Pager.png, zuletzt abgerufen am 16.6.2019.

7 Stand 16.6.2019.

8 https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/OH_TMG.pdf, zuletzt abgerufen am 16.6.2019.

9 Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, S. 12, https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/OH_TMG.pdf, zuletzt abgerufen am 16.6.2019.

10 Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, S. 13, https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/OH_TMG.pdf, zuletzt abgerufen am 16.6.2019.

ein Pseudonym per Cookie zugewiesen, der Nutzer wird außerdem über die Verarbeitungen seiner Daten in der Datenschutzerklärung informiert und ihm wird schließlich die Möglichkeit gegeben, nach Art. 21 Abs. 1 DS-GVO Widerspruch gegen die Verarbeitung der Daten einzulegen. Darüber hinaus findet keine Verknüpfung mit anderen Daten (von Google) statt.

Sobald allerdings etwa die IP-Adresse verarbeitet wird oder eine Verknüpfung mit einer eindeutigen ID oder mit weiteren Daten von Google stattfindet, überwiegt das Interesse des Nutzers und eine Einwilligung ist erforderlich.

7 Verarbeitung auf Grundlage von Art. 6 Abs. 1 S. 1 lit. a DS-GVO

Entscheidet sich der Betreiber einer Webseite dafür, eine Einwilligung einzusetzen, kommt er kaum am Einsatz eines Cookie-Banners vorbei. Hierbei begegnet der Betreiber einigen Hürden, an der eine beträchtliche Zahl der aktuell eingesetzten Cookie-Banner scheitert. Angefangen damit, dass viele Cookie-Banner keine Wahlmöglichkeit bieten und somit keine unmissverständliche Zustimmung erkennen lassen, scheitern andere daran, dass hier ein bloßes Weiterscrollen als konkludente Einwilligung ausgelegt wird. Beides erfüllt nicht die Anforderungen des Art. 4 Nr. 11 DS-GVO, wonach eine „unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung“ vorliegen muss.

Hat das Cookie-Banner die erste Hürde genommen, steht es unmittelbar vor der zweiten: Das Tracking darf erst dann beginnen, wenn der Nutzer seine Einwilligung erklärt hat. In vielen Fällen sind Cookie-Banner aber einfach gehaltene Ebenen, die technisch nichts anderes tun, als ein Cookie anzulegen, aus dem hervorgeht, dass der Nutzer das Banner „weggeklickt“ hat oder dass er zugestimmt, bzw. nicht zugestimmt hat. Einzige Folge daraus ist oft, dass das Cookie-Banner beim nächsten Besuch nicht mehr angezeigt wird. Das eigentliche Tracking-Script von Google Analytics oder Matomo ist in diesen Fällen von dem Banner völlig unabhängig, legt Cookies an und verfolgt den Benutzer, ohne dass eine entsprechende Einwilligung des Nutzers vorliegt. Ganz zu schweigen davon, dass in diesem Fall regelmäßig nur im Browser des Besuchers (per Cookie) protokolliert wird, ob der Besucher eingewilligt hat. Der Betreiber der Seite kann in diesem Fall also ohne den Browser des Nutzers seinen Nachweispflichten nach Art. 7 Abs. 1 DS-GVO nicht nachkommen, da lediglich dort gespeichert wird, ob der Nutzer eingewilligt hat. Solange er das an den Server mitgesendete Cookie, aus dem die Entscheidung des Nutzers hervorgeht, nicht speichert, fehlt ihm die Nachweismöglichkeit.

Eine datenschutzkonforme Implementierung der Einwilligung zum Tracking setzt vielmehr voraus, dass die Ausführung des Tracking-Codes an die Voraussetzung geknüpft ist, dass der Nutzer seine Einwilligung erteilt hat. Das lässt sich in der Praxis mit einem entsprechenden JavaScript-Code realisieren, der den Eintrag im „Cookie-Banner“-Cookie prüft und entsprechend des Eintrags den Tracking-Code ausführt oder aber verhindert. Daneben muss für den Nutzer auch noch eine Möglichkeit geschaffen werden, seine Einwilligung zu widerrufen, indem er etwa das Cookie-Banner erneut aufrufen und Einstellungen verändern kann, was ebenso oft vergessen wird.

8 Tracking ohne Cookies

Alternativ dazu, dass Tracking-Informationen im Cookie gespeichert werden, kann ein Besucher außerdem per (aktivem) Browser-Fingerprinting nachverfolgt werden. Hierzu erstellt das Tracking-Script einen Fingerabdruck (sogenannter Fingerprint) des Browsers des Besuchers. Beim aktiven Fingerprinting wird beispielsweise ein Wert daraus errechnet, welche Auflösung, welches Betriebssystem, welche Schriftarten oder welche Zeitzone das Gerät des Besuchers hat. Hierdurch lässt sich eine erhebliche Zahl der Nutzer wiedererkennen. Beim passiven Fingerprinting hingegen werden (ohne Zuhilfenahme von JavaScript) auf Serverseite die Informationen ausgewertet, die der Browser bei seiner Anfrage ohnehin mitschickt. Überträgt man das zuvor Ausgeführte auf ein Cookie-loses Tracking, so lässt sich für den Fall, dass ein Fingerprinting mit einer anonymisierten IP-Adresse stattfindet, eine vergleichbare Lage wie bei der zurückhaltenden Implementierung von Google Analytics feststellen. Ein solches Cookie-loses Tracking auf Basis eines zurückhaltenden Fingerprints ohne Verarbeitung der IP-Adresse lässt sich beispielsweise bei Matomo direkt konfigurieren.

9 Fazit

Auch wenn der Trend zu immer mehr Cookie-Bannern geht, lässt sich zum einen festhalten, dass nicht für jedes Tracking ein Cookie-Banner nötig ist, zum anderen lässt sich feststellen, dass eine Vielzahl von Cookie-Bannern in Deutschland gar nicht notwendig sind. Vielmehr wird, offenbar aus Sorge vor Bußgeldern, sofort zum Cookie-Banner gegriffen, selbst wenn ein solches gar nicht erforderlich ist. Wohl auch aus diesen Gründen wird zu Unrecht mit Cookies fast ausschließlich Tracking oder Werbung in Verbindung gebracht.