Der Bayerische Landesbeauftragte
für den Datenschutz

Cookie-Einwilligungen auf Webseiten bayerischer öffentlicher Stellen

Aktuelle Kurz-Information 36

Stichwörter: Cookies – Einwilligung – Einwilligungsbanner – ePrivacy-Richtlinie – Internet-Browsereinstellungen – Telemedien – Webseiten – Widerspruchsrecht | **Stand:** 1. Oktober 2021

Viele Webseiten verwenden Cookies – kleine Datensätze, die auf dem Endgerät der Nutzerin oder des Nutzers (etwa Smartphone, Notebook, PC) beim Besuch von Webseiten gespeichert werden. Nutzerinnen und Nutzer erkennen deren Einsatz vor allem an den Hinweis- oder Einwilligungsbannern, die beim Aufruf von Webseiten erscheinen. Regelmäßig werden ihnen mittels komplexer Formulare viele Entscheidungen zum Einsatz einzelner Cookies abverlangt, ehe eine Webseite mit allen ihren Funktionen zur Verfügung steht. Auch bei Webseiten bayerischer öffentlicher Stellen werden Nutzerinnen und Nutzer damit konfrontiert. In diesem Zusammenhang stellt sich häufig die Frage, wie sich der Einsatz von Cookies einschränken oder vermeiden lässt. Aus datenschutzrechtlicher Sicht ist hierzu Folgendes zu bemerken:

1. Was sind und wie funktionieren Cookies?

Wird eine Webseite besucht, kann sie beispielsweise diese Information im jeweils genutzten Browser in einer Zeichenkette (Cookie) speichern. Beim erneuten Besuch sendet der Browser den gespeicherten Inhalt zurück an die Webseite. Wurde beim ersten Besuch etwa eine eindeutige Nummer zugewiesen und in einem Cookie gespeichert, können Nutzerinnen und Nutzer mit Hilfe dieses Cookies wiedererkannt werden.

Cookies können von der Betreiberin oder dem Betreiber der besuchten Webseite (sogenannte First-Party-Cookies) oder von Dritten (sogenannte Third-Party-Cookies) gesetzt werden. Sie können zu einer nutzerfreundlichen Bedienung der Webseite beitragen, indem sie beispielsweise Einstellungen der Nutzerinnen und Nutzer – wie die gewünschte Sprache oder sonstige Präferenzen – speichern. So muss die Nutzerin oder der Nutzer die Webseite nicht bei jedem Besuch erneut individuell anpassen. Zugleich ermöglichen Cookies etwa die Erstellung von Statistiken: Nutzungsprofile können angelegt und das Nutzungsverhalten kann ausgewertet werden, was insbesondere für das Online-Marketing von Webseitenbetreiberinnen und -betreibern und gegebenenfalls ihrer Geschäftspartnerinnen und -partner von großer Bedeutung ist.

Grundsätzlich unterscheidet man zwischen (technisch) notwendigen und optionalen (nicht notwendigen) Cookies.

Zu den notwendigen Cookies gehören solche, die eine Webseite erst nutzbar machen oder ausschließlich der IT-Sicherheit dienen. Dies ist bei den sogenannten Session-Cookies in der

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18 | Telefon: +49 89 21 26 72-0
poststelle@datenschutz-bayern.de | https://www.datenschutz-bayern.de

Regel der Fall. Sie speichern temporär unter anderem Log-in-Daten oder Spracheinstellungen und machen dadurch die erneute (möglicherweise ansonsten nach wenigen Sekunden notwendige) Anmeldung an den Webseiten entbehrlich. Mit dem Schließen des Browsers werden sie automatisch gelöscht. Aber auch dauerhafte Cookies können für das Funktionieren einer Webseite erforderlich sein, wie etwa Cookies, welche die in den Einwilligungsbannern vorgenommenen Einstellungen speichern.

Nicht notwendige Cookies sind vor allem solche, die das Verhalten von Nutzerinnen und Nutzern im Internet zu Marketingzwecken (dauerhaft) verfolgen (sog. Tracking-Cookies). Aber auch Cookies, die der statistischen Auswertung oder der Webseitenanalyse dienen, sind – selbst wenn sie für die Verbesserung der Webseitenangebote nützlich sein können – als nicht erforderlich anzusehen.

2. Gesetzliche Ausgangslage

Anbieter von Telemediendiensten (wie Webseitenbetreiber, Anbieter von Smartphone-Apps) haben beim Einsatz von Cookies nicht nur die Vorgaben des Telekommunikations- und Telemedienrechts zu beachten. Bei der Verarbeitung personenbezogener Daten sind sie als Verantwortliche im Sinne von Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) auch an deren Bestimmungen gebunden.

a) Vorgaben der ePrivacy-Richtlinie

Bereits das erstmalige Speichern von Daten mittels Cookies auf einem Endgerät bedarf nach der Rechtsprechung des Bundesgerichtshofs grundsätzlich einer Einwilligung der Nutzerin oder des Nutzers.[1] Diese Vorgabe folgt allerdings nicht aus der Datenschutz-Grundverordnung, sondern aus der Regelung des Art. 5 Abs. 3 Richtlinie 2002/58/EG[2] in der Fassung der Richtlinie 2009/136/EG[3] (ePrivacy-Richtlinie). Danach ist auch der Zugriff auf Informationen einwilligungsbedürftig, die bereits im Endgerät der Nutzerin oder des Nutzers gespeichert sind. Von diesem Erfordernis sind nach Art. 5 Abs. 3 Satz 2 ePrivacy-Richtlinie (technisch) notwendige Cookies ausgenommen. Art. 5 Abs. 3 ePrivacy-Richtlinie schützt primär die Integrität des Geräts und ist auch dann anwendbar, wenn keine personenbezogenen Daten verarbeitet werden.

Gesetzliche Neuregelung: Am 1. Dezember 2021 tritt das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) in Kraft. Mit § 25 TTDSG setzt der Gesetzgeber die Vorgaben von Art. 5 Abs. 3 ePrivacy-Richtlinie um und schreibt nun ausdrücklich auf nationaler Ebene die grundsätzliche Einwilligungsbedürftigkeit des Einsatzes von Cookies vor. Die derzeitige richtlinienkonforme Auslegung von § 15 Abs. 3 Telemediengesetz (TMG) wird damit bestätigt. Die Zahl der in der Praxis einzuholenden Einwilligungen dürfte sich daher nicht signifikant verändern.

b) Vorgaben der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung dient vorrangig dem Schutz personenbezogener Daten. Aufgrund dieses (anderen) Schutzzwecks ist sie neben den Regelungen der ePrivacy-Richtlinie anwendbar, soweit personenbezogene Daten verarbeitet werden.

Erhebt eine Webseitenbetreiberin oder ein Webseitenbetreiber Nutzungsdaten mittels Einsatzes von Cookies und übermittelt sie oder er diese gegebenenfalls an Dritte (etwa zu Trackingzwecken), bedürfen diese Verarbeitungen personenbezogener Daten jeweils einer gesonderten datenschutzrechtlichen Erlaubnis, die nicht zwingend in einer Einwilligung bestehen muss.

In der Regel stützen sich öffentliche Stellen als Webseitenbetreiberinnen und -betreiber aber auf Einwilligungen der Nutzerinnen und Nutzer (aus Datenschutzsicht: der betroffenen Personen). Die Einwilligung ist gemäß Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Anders als nichtöffentliche Stellen können sich öffentliche Webseitenanbieterinnen und -anbieter, die Daten in Erfüllung ihrer Aufgaben verarbeiten, wegen Art. 6 Abs. 1 UAbs. 2 DSGVO nicht auf Art. 6 Abs. 1 UAbs. 1 Buchst. f DSGVO berufen. Auch eine vertragliche Grundlage gemäß Art. 6 Abs. 1 Buchst. b DSGVO kommt kaum in Betracht. Rechtsbeziehungen zwischen Nutzerinnen und Nutzern auf der einen und öffentlichen Stellen auf der anderen Seite sind meist nicht vertraglich ausgestaltet. Im Übrigen dürfte es an der objektiven Erforderlichkeit der Verarbeitung der unter Einsatz von Cookies zu erhebenden Daten für die Erfüllung des Vertrags fehlen, Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO.

Beispiel 1: Die Stadtwerke A. GmbH – ein Beteiligungsunternehmen der Stadt A. – betreibt unter anderem eine Wasserversorgungsanlage. Eine Bürgerin möchte Wasser von der Stadtwerke A. GmbH beziehen. Um den Vertrag zu erfüllen, muss die Stadtwerke A. GmbH unter anderem die zu beliefernde Adresse und Zahlungsinformationen der Bürgerin zu Liefer- und Abrechnungszwecken nach Art. 6 Abs. 1 UAbs. 1 Buchst. b DSGVO verarbeiten. Diese Daten gibt die Bürgerin auf der Webseite der Stadtwerke A. GmbH in ein Antragsformular ein.

Möchte die Stadtwerke A. GmbH zugleich eine Analyse ihrer Webseite aufgrund des Verhaltens der Webseitennutzerin (unter Einsatz von Cookies) vornehmen, ist dies nicht mehr für die Durchführung des Vertrages erforderlich. Selbst wenn die Webseitenanalyse im Vertrag ausdrücklich erwähnt wird, hängt der Abschluss des Vertrages nicht davon ab.

3. Notwendigkeit der „Einwilligungsbanner“

Die Einwilligungsbedürftigkeit solcher Datenverarbeitungen, sei es nach der ePrivacy-Richtlinie, sei es aufgrund der Datenschutz-Grundverordnung, macht nach derzeitiger Gesetzeslage den Einsatz einer Vielzahl von sog. „Einwilligungsbannern“ erforderlich. Auch wenn die Kritik an der Vielzahl der „Einwilligungsbanner“ und ihrer Komplexität verständlich ist, fehlen doch – jedenfalls derzeit – echte praktikable Alternativen zum Einholen von Einwilligungen.

Gesetzliche Neuregelung: Das Telekommunikation-Telemedien-Datenschutz-Gesetz soll die Position der Nutzerinnen und Nutzer bei der Kontrolle über die erteilten Einwilligungen,

mithin über die Verarbeitung der eigenen personenbezogenen Daten stärken. § 26 Abs. 2 TTDSG schafft hierzu eine Verordnungsermächtigung für Regelungen zur Einführung zentraler Dienste des Einwilligungsmanagements. Gegenstand sollen Verfahren und technische Anwendungen zur Einholung und Verwaltung der Einwilligungen sein. Ob sich solche Lösungen durchsetzen und als Mehrwert für die Nutzerinnen und Nutzer erweisen werden, bleibt abzuwarten.

Erfordert eine Verarbeitung personenbezogener Daten unter Einsatz von Cookies keine Einwilligung nach Maßgabe von Art. 5 Abs. 3 ePrivacy-Richtlinie und kann diese Datenverarbeitung aufgrund einer anderen datenschutzrechtlichen Rechtsgrundlage durchgeführt werden, ist der Einsatz von „Einwilligungsbannern" nicht erforderlich, nach meiner Einschätzung jedoch unschädlich. Dies dürfte in der Regel bei sogenannten notwendigen Cookies (siehe oben 1.) der Fall sein.

Die einfachste Lösung, auf Einwilligungsbanner verzichten zu können, liegt darin, keine Cookies zu verwenden. Bereits bei der Neugestaltung von Webseiten sollte kritisch geprüft werden, wie viele und welche Cookies tatsächlich notwendig sind. Das entspricht auch dem Grundsatz der Datenminimierung (vgl. Art. 5 Abs. 1 Buchst. c DSGVO).

4. Anforderungen an eine Einwilligung

Die mittels „Einwilligungsbannern" eingeholte Einwilligung für eine Verarbeitung personenbezogener Daten ist nur dann wirksam, wenn sie die Anforderungen erfüllt, welche Art. 6 Abs. 1 UAbs. 1 Buchst. a, Art. 4 Nr. 11 und Art. 7 DSGVO vorsehen. Über diese Anforderungen informiert meine Orientierungshilfe „Die Einwilligung nach der Datenschutz-Grundverordnung".[4] Für die nach Maßgabe von Art. 5 Abs. 3 ePrivacy-Richtlinie einzuholende Einwilligung gelten gemäß Art. 2 Satz 2 Buchst. f ePrivacy-Richtlinie in Verbindung mit Art. 94 Abs. 2 Satz 1 DSGVO insbesondere die Bestimmungen der Datenschutz-Grundverordnung zur Definition der Einwilligung entsprechend.

Eine Einwilligung muss danach insbesondere freiwillig (Art. 4 Nr. 11 DSGVO), informiert (Art. 4 Nr. 11 DSGVO), auf einen bestimmten Zweck (Art. 6 Abs. 1 UAbs. 1 Buchst. a DSGVO) und auf eine bestimmte Verarbeitung bezogen (Art. 4 Nr. 11 DSGVO) sowie unmissverständlich (Art. 4 Nr. 11 DSGVO) sein. Sie wirkt grundsätzlich bis zu ihrem Widerruf (Art. 7 Abs. 3 Satz 1 und 2, Abs. 4 DSGVO). Für den Einsatz der „Einwilligungsbanner" bedeutet dies insbesondere, dass

- ein aktives Tun der Nutzerin oder des Nutzers, etwa durch Ankreuzen oder Anklicken eines Kästchens, vorausgesetzt wird;
- keine Daten erhoben und weitergegeben werden dürfen, bevor eine Einwilligung durch die Nutzerin oder den Nutzer erteilt wurde (sog. Opt-In-Lösung);

  Beispiel 2: Zum Online-Abschluss eines Vertrages verlangt die Stadtwerke A. GmbH durch ein permanent angekreuztes Kästchen die Einwilligung zu einer Webseitenanalyse. Diese Vorgehensweise erfüllt nicht die Anforderungen an eine Opt-In-Lösung und

dürfte zugleich einen Verstoß gegen das Koppelungsverbot (Art. 7 Abs. 4 DSGVO) darstellen;

- klar und deutlich anzugeben ist, welche Daten erhoben werden, an wen (namentlich) sie gegebenenfalls weitergegeben werden und zu welchem Zweck dies geschieht;
- die Ausübung des Widerrufsrechts jederzeit gewährleistet sein muss und ein Widerruf genauso einfach durchzuführen sein muss wie die Einwilligungserklärung selbst. Wird die Einwilligung widerrufen, berührt dies die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung (beispielsweise einer Datenübermittlung an Dritte) jedoch nicht, Art. 7 Abs. 3 Satz 2 DSGVO.

5. Schutz vor ungewolltem Cookie-Einsatz

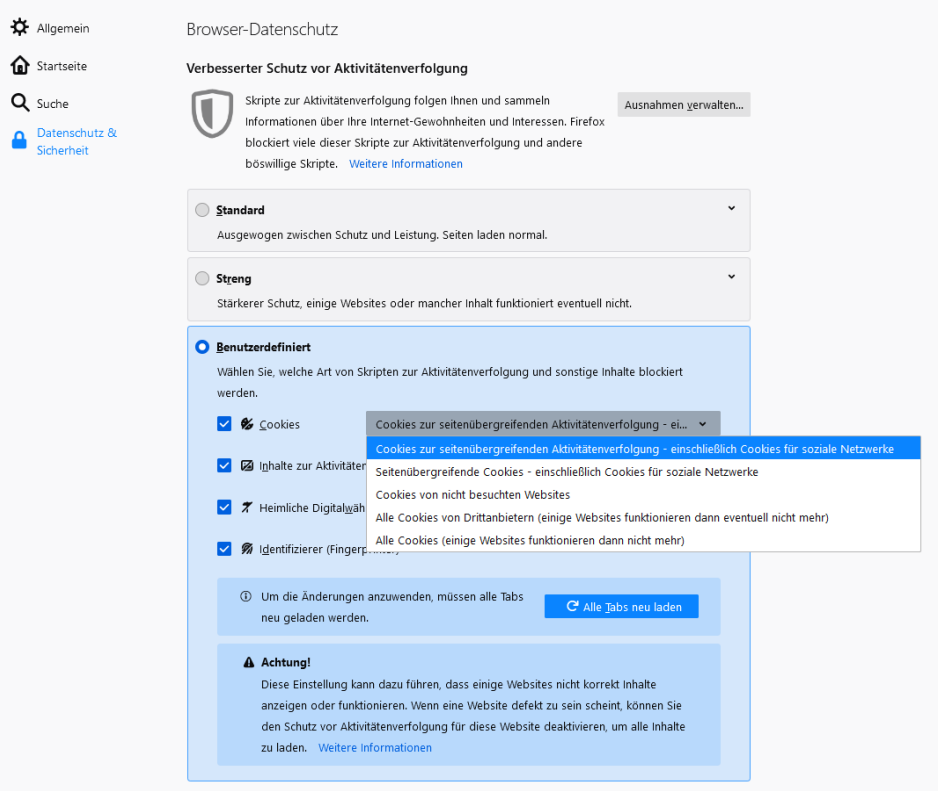
Zur Begrenzung des Einsatzes von Cookies sind auch die Nutzerinnen und Nutzer von Webseiten selbst gefordert. Auch wenn Webseitenbetreiberinnen und -betreiber mitunter recht kreative Lösungen entwickeln, um eine Begrenzung des Cookie-Einsatzes zumindest kompliziert zu gestalten, ist eine Abwahl der nicht notwendigen Cookies meist möglich.

Nutzerinnen und Nutzer können die Filterung und Speicherung von Cookies zudem durch entsprechende Einstellungen in ihrem jeweiligen Internet-Browser steuern. Anleitungen zu den Konfigurationsmöglichkeiten der einzelnen Browser sowie zur systemspezifischen Umsetzung allgemeiner Handlungsempfehlungen finden sich im Internet, etwa bei der Verbraucherzentrale Bundesverband[5], bei der Stiftung Warentest[6] oder beim Bundesamt für Sicherheit in der Informationstechnik.[7] Dort werden beispielhaft folgende Hinweise gegeben:

- Cookies können durch entsprechende Browser-Einstellungen im Vorhinein zugelassen oder gesperrt werden. Zwar bieten nicht alle Browser gleiche Schutzmechanismen; meistens kann aber eingestellt werden, dass dauerhafte Cookies automatisch nach jedem Schließen des Browsers gelöscht werden. Session-Cookies werden ohnehin automatisch gelöscht.

  Erläuterung am Beispiel von Firefox:

  1. Klicken Sie links von der Adressleiste auf das Schildsymbol und wählen Sie „Schutzmaßnahmen-Einstellungen“. Danach öffnen sich die Firefox-Einstellungen des Abschnitts „Datenschutz & Sicherheit“ in einem neuen Tab.
  2. Aktivieren Sie die Option „Benutzerdefiniert“.
  3. Nachdem Sie das Häkchen bei „Cookies“ gesetzt haben, können Sie zwischen verschiedenen Optionen wählen, je nachdem, welche Cookies blockiert werden sollen.
  4. Klicken Sie abschließend auf die Schaltfläche „Alle Tabs neu laden“, damit die vorgenommenen Änderungen wirksam werden.



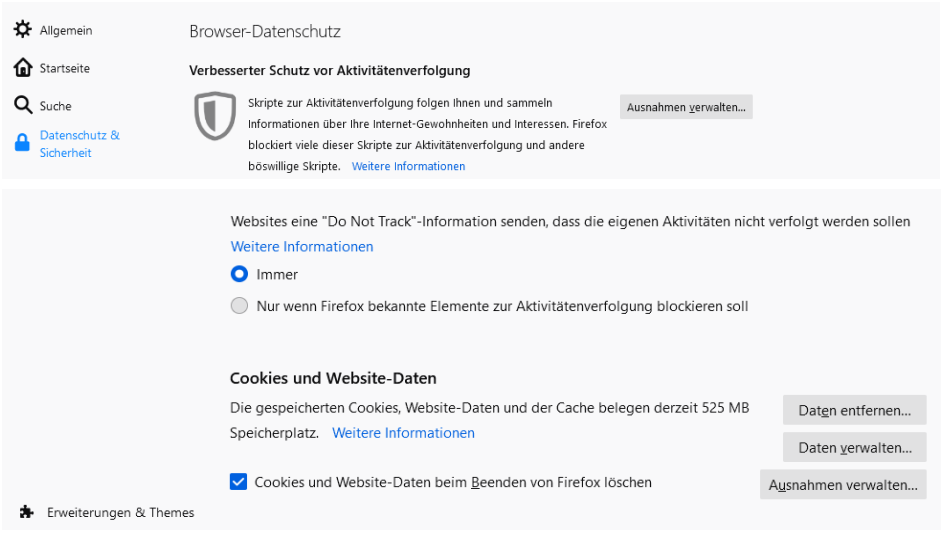
- Nutzerinnen und Nutzer können zudem im Browser die Cookies von Dritten generell deaktivieren. Dies dürfte meist die Funktionalität der Webseiten nicht einschränken, da solche Cookies regelmäßig zum Online-Marketing (Tracking) eingesetzt werden.

- Zudem können Nutzerinnen und Nutzer bestimmte technische Voreinstellungen an ihren Endgeräten vornehmen (zum Beispiel „Do Not Track“ oder ein „Incognito-Modus“).

- Cookies lassen sich durch spezielle Systemfunktionen auch im Nachhinein löschen. Daher können Cookies, die aufgrund der Browserkonfiguration nicht blockiert werden, regelmäßig gelöscht werden. Diese Löschfunktionalität ist meist über die Einstellungen des Browsers oder auf den Geräten unter „Datenschutz“ oder „Inhaltseinstellungen“ zu finden. Machen Sie es sich zur Gewohnheit, Cookies, die Sie nicht bewusst nutzen möchten, zumindest einmal im Monat zu löschen.

  Erläuterung am Beispiel von Firefox:

  1. Klicken Sie links von der Adressleiste auf das Schildsymbol und wählen Sie „Schutzmaßnahmen-Einstellungen“. Danach öffnen sich die Firefox-Einstellungen des Abschnitts „Datenschutz & Sicherheit“ in einem neuen Tab.
  2. Hier können Sie nach den oben erwähnten Einstellungen unter anderem die Optionen „Do Not Track“ und „Cookies und Website-Daten beim Beenden von Firefox löschen“ auswählen.



Um sich einen Überblick über die Vielzahl der Unternehmen, die beim Besuch einer Webseite Cookies setzen, zu verschaffen und den Einsatz von Cookies entsprechend einzuschränken, kann die Verwendung eines Anti-Tracking-Add-ons sinnvoll sein.

Hinzuweisen ist schließlich darauf, dass Art. 21 Abs. 2 DSGVO den betroffenen Personen ein voraussetzungsloses Widerspruchsrecht einräumt, wenn personenbezogene Daten – etwa zwecks Direktwerbung – verarbeitet wurden. Das gleiche gilt auch für ein Profiling im Zusammenhang mit Direktwerbung.

1 Bundesgerichtshof, Urteil vom 28. Mai 2020, I ZR 7/16, NJW 2020, 2540, Rn. 47 ff.

2 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre in der elektronischen Kommunikation (ABl. L 201 vom 31. Juli 2002, S. 37, ber. ABl. L 241 vom 10. September 2013, S. 9, und ABl. L 162 vom 23. Juni 2017, S. 56).

3 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25.11.2009 (ABl. L 337 vom 18. Dezember 2009, S. 11).

4 Bayerischer Landesbeauftragter für den Datenschutz, Die Einwilligung nach der Datenschutz-Grundverordnung, Stand 9/2021, Internet: https://www.datenschutz-bayern.de, Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Einwilligung".

5 Verbraucherzentrale Bundesverband, Cookies kontrollieren und verwalten, Stand: 2/2021, Internet: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/cookies-kontrollieren-und-verwalten-11996.

6 Stiftung Warentest, Cookies löschen, Browser richtig einstellen, Stand: 11/2020, Internet: https://www.test.de/Sicher-surfen-Cookies-loeschen-Browser-richtig-einstellen-4418201-0.

7 Bundesamt für Sicherheit in der Informationstechnik, Cookies und Fingerprints verhindern, Stand: 9/2021, Internet: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Updates-Browser-Open-Source-Software/Der-Browser/JavaScript-Cookies-Fingerprints/javascript-cookies-fingerprints.