UMSETZUNG DER COOKIE-RICHTLINIE – STATUS QUO

Mareike Papendorf, Niels Lepperhoff

Die Nutzung von Cookies stellt Webseitenbetreiber oft vor unerwartete Schwierigkeiten. Die sich aus europäischem und deutschem Recht ergebenen Anforderungen stoßen in der Praxis auf Umsetzungshürden, wie z. B. die Pflicht zur Protokollierung von Einwilligungen. Auch die technische Umsetzung von obligatorischen Widerspruchsmöglichkeiten birgt juristische Stolpersteine. Für internationale Webseiten kommt erschwerend hinzu, dass es keine einheitliche Rechtslage innerhalb der EU gibt. Für ausgewählte Ländern werden die nationalen Umsetzungen der Richtlinie 2009/136/EG (»Cookie-Richtlinie«) vorgestellt.

Einleitung

Cookies sind aus dem Internet nicht mehr wegzudenken. Viele Webseiten nutzen sie zur Session-Steuerung. Webstatistiken erkennen mit Hilfe von Cookies wiederkehrende Besucher. In der Online-Werbung helfen Cookies bereits ausgespielte Anzeigen zu erkennen. Dennoch haben es sowohl der deutsche als auch der europäische Gesetzgeber versäumt, eindeutige Rahmenbedingungen für die Nutzung von Cookies zu schaffen. Ein Ende der damit verbundenen Unsicherheit wird es auch durch die Datenschutz-Grundverordnung, die voraussichtlich Anfang 2018 in Kraft treten wird, nicht geben. Dieser Artikel beschreibt die aktuelle rechtliche Situation der Nutzung von Cookies und bietet einen Ausblick über mögliche Entwicklungen. Daneben werden der praktische Einsatz von Cookies in Deutschland, Österreich und Großbritannien und Alternativen für die Erstellung von Webstatistiken betrachtet. ▸

Anwendungsbereich der Cookie-Richtlinie

Am 19.12.2009 trat die Richtlinie 2009/136/EG, die meist als »Cookie-Richtlinie« bezeichnet wird, in Kraft. Sie regelt die Bereitstellung elektronischer Kommunikationsnetze und -dienste für Endnutzer. Die Cookie-Richtlinie enthält unter anderem Vorschriften über die Speicherung von Informationen auf Endgeräten und den Zugriff auf diese (Art. 2 der Cookie-Richtlinie, der damit Art. 5 Abs. 3 der Richtlinie 2002/58/EG ändert). Solche Speicherungen und Zugriffe dürfen laut der Richtlinie nur mit Einwilligung des Nutzers erfolgen, welche auf der Basis von klaren und umfassenden Informationen erteilt werden muss. Eine Einwilligung ist entbehrlich, wenn die Speicherung oder der Zugriff alleine für die Übertragung einer Nachricht oder zur Nutzung eines Dienstes, den der Nutzer ausdrücklich gewünscht hat, erforderlich ist.

Von diesen Regelungen sind sowohl Browser-Cookies als auch Flash-Cookies betroffen, da sie zum einen auf Endgeräten der Nutzer gespeichert werden und zum anderen ein Zugriff auf die im Cookie enthaltenen Informationen möglich ist. In beiden Arten von Cookies können verschiedenste Informationen hinterlegt werden, denn sie können einen beliebigen Text enthalten. Um zu beurteilen, für welche Cookies eine Einwilligung benötigt wird, muss zwischen den Aufgaben, die die Cookies wahrnehmen sollen, unterschieden werden. Cookies werden hauptsächlich verwendet als:

- Komfort-Cookies für persönliche Einstellungen wie z. B. Login-Daten oder Spracheinstellungen,
- Session-Cookies, die zur Steuerung einer Webseite benötigt werden und
- Tracking-Cookies zur Erstellung von Webstatistiken

Session-Cookies werden zur Steuerung einer Webseite benötigt und sind für die Nutzung des Dienstes erforderlich. Die Richtlinie 2002/58/EG sieht für diese Cookies keine Pflicht zur Einholung einer Einwilligung vor.

Eine vergleichbare Regelung findet sich für die Nutzung von Telemediendiensten, wozu auch Webseiten gehören, im deutschen Telemediengesetz (TMG). Diese besagt, dass Anbieter von Telemediendiensten die personenbezogenen Daten ihrer Nutzer erheben und verwenden, wozu auch speichern gehört, dürfen, wenn dies erforderlich ist, um die Nutzung des Dienstes zu ermöglichen (§ 15 Abs. 1, S. 1 TMG). Diese Vorschrift lässt jedoch offen, ob sie sich nur auf den Einflussbereich des Diensteanbieters bezieht oder auch auf den Einflussbereich des Nutzers und damit auch für die Speicherung von Dateien auf seinem Endgerät gilt, die der Nutzer selber steuern kann.[4]

Sowohl Komfort- als auch Tracking-Cookies sind weder für die Übertragung von Nachrichten noch für die Nutzung von Diensten erforderlich. Deshalb sieht die Cookie-Richtlinie die Einholung einer Einwilligung für deren Speicherung und den Zugriff auf sie vor.

Im TMG finden sich jedoch keine Vorschriften, die speziell auf Komfort-Cookies eingehen. Das Gesetz erlaubt jedoch die Erhebung und Verwendung von personenbezogenen Daten der Nutzer, wenn diese ihre Einwilligung erteilt haben (§ 12 Abs. 1 und 2 TMG). Ob von dieser Regelung Komfort-Cookies umfasst sind, ist unklar. Auch diese Vorschrift lässt offen, ob sie sich nur auf den Einflussbereich des Diensteanbieters bezieht oder auch auf den Einflussbereich des Nutzers und damit auch für die Speicherung von Komfort-Cookies auf seinem Endgerät gilt.

Dieser Text bezieht sich im Folgenden auf Tracking-Cookies, weil diese in der Praxis am häufigsten vorkommen.

Hürden der Einholung einer Einwilligung

Für Tracking-Cookies sieht die Cookie-Richtlinie eine Pflicht zur Einholung einer Einwilligung vor. Daher stellt sich die Frage, wie die Einholung einer Einwilligung technisch umgesetzt werden kann.

In der Praxis wird zuweilen von einer konkludenten Einwilligung durch die Nutzung eines Dienstes, etwa dem Besuch einer Webseite, ausgegangen. Die Ausführungen des BDSG lassen eine konkludente Einwilligung im Regelfall jedoch nicht zu. Es kann zwar auf die Schriftform der Einwilligung verzichtet werden, wenn »wegen besonderer Umstände eine andere Form ange-

[4] Zscherpe in Taeger/Gabel (2010): § 15 TMG, Rn. 33 f. unterstellt die Anwendbarkeit dieser Vorschrift für das Setzen von Cookies auf dem Computer des Nutzers wenig überzeugend ohne nähere Begründung.

messen ist« (§ 4a Abs. 1, S. 3 BDSG). Doch ist mit dieser »anderen Form« aus Sicht der Aufsichtsbehörden eine ausdrückliche, mündliche und nicht etwa konkludente Einwilligung gemeint.[5] Zudem erfüllt eine konkludente Einwilligung auch weder die inhaltlichen Voraussetzungen des BDSG noch die des TMGs, die bei Telemediendiensten vorrangig anwendbar sind. So kann eine konkludente Einwilligung nicht protokolliert werden, wie es § 28 Abs. 3a, S. 1 BDSG und § 13 Abs. 2, Nr. 2 TMG bei elektronisch erklärten Einwilligungen fordern. Auch andere Anforderungen wie die des Wissen des Nutzers über den Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten (§ 4a Abs. 1, S. 1 BDSG) oder das Vorliegen einer bewussten und eindeutigen Einwilligung (§ 13 Abs. 2, Nr. 1 TMG) werden durch eine konkludente Einwilligung nicht erfüllt. Dies gilt auch dann, wenn entsprechende Informationen auf einer Webseite angezeigt werden, da nicht sicher ist, ob der Nutzer diese zur Kenntnis genommen und verstanden hat.

Die Voraussetzungen und Folgen sowie die Verpflichtungen, die im Zusammenhang mit der Einholung einer Einwilligung gelten, werden zukünftig durch die Datenschutz-Grundverordnung (im Folgenden als »DS-GVO« bezeichnet) geregelt. Dieser Artikel bezieht sich im Folgenden auf den Stand der Datenschutz-Grundverordnung vom 15.12.2015, die vom Innen- und Justizausschuss des EU-Parlaments angenommen wurde, aber noch vom Ministerrat und dem Plenum des EU-Parlaments offiziell beschlossen werden muss, damit sie im Amtsblatt der EU verkündet werden kann und damit Gültigkeit erlangt. Nach derzeitigem Kenntnisstand werden sich an den wesentlichen Merkmalen der Einwilligung keine Änderungen ergeben.

Es ist jedoch unklar, ob die DS-GVO die Möglichkeit einer konkludenten Einwilligung zulassen wird. Die DS-GVO definiert in Art. 4 (8), dass eine Einwilligung als »… statement or by a clear affirmative action …« abgeben werden muss. Daher ist nach diesem Wortlaut auch eine konkludente Einwilligung denkbar. Allerdings wird in Art. 7 (1) DS-GVO gefordert, dass »… the controller shall be able to demonstrate the consent was given by the data subject …« Diese Nachweispflicht dürfte in vielen Fällen eine konkludente Einwilligung ausschließen. Dies gilt auch für eine konkludente Einwilligung durch den Besuch einer Webseite, die durch den Webseitenbetreiber ohne Identifikation des Nutzers und eine entsprechende Protokollierung nicht nachgewiesen werden kann.

Sobald Nutzer ohne Identifikation einwilligen, läuft eine aussagekräftige Protokollierung ins Leere. Eine Identifizierung ausschließlich zum Zwecke der Protokollierung steht vor rechtlichen und Akzeptanzhürden. Rechtlich schwierig wäre auch der Zwang einer namentlichen Anmeldung. Beispielhaft sei darauf hingewiesen, dass Telemediendienste anonym oder unter einem Pseudonym nutzbar sein müssen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6, S. 1 TMG). Davon abgesehen dürften Webseiten durch einen Anmeldezwang eher Besucher verlieren als gewinnen.

Für Nutzer, die sich vor der Abgabe ihrer Einwilligung z. B. durch Anmeldung an der Webseite identifiziert haben, lässt sich die Abgabe der Einwilligung einfach protokollieren. Dazu ist lediglich ein Eintrag in eine Datenbank, bestehend aus Nutzername, Einwilligung und Zeitstempel, notwendig.

Allerdings kann auf die namentliche Anmeldung verzichtet werden, wenn dem Benutzer ein Pseudonym zu Identifikationszwecken zugeordnet werden kann. Das in der Onlinewerbung zum Wiedererkennen von Besuchern verwendete Fingerprinting (vgl. 1.4) leistet eine solche Identifizierung nicht, da verschiedene – mithin tausende – Besucher den gleichen Fingerprint erhalten.

Das Double-Opt-in kann eine Identifizierung des Nutzers ermöglichen. In der Praxis wird hierbei im ersten Schritt oft eine E-Mail mit einem Bestätigungslink an die angegebene Kontaktadresse versandt. Erst wenn im zweiten Schritt der Nutzer die Kontaktadresse durch Klicken des Bestätigungslinks aktiviert, gilt die Einwilligung als erteilt. Die Einwilligung kann eindeutig einer E-Mail-Adresse zugeordnet und protokolliert werden. Der BGH hält das Double-Opt-in bei E-Mails grundsätzlich für geeignet, um das Vorliegen einer Einwilligung nachweisen zu können.[6] ▸

[5] Innenministerium Baden-Württemberg (2007): Vierter Tätigkeitsbericht des Innenministeriums nach § 39 des Landesdatenschutzgesetzes 2007. URL: *http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/4.-Tätigkeitsbericht-des-Innenministeriums-2007.pdf*. Letzter Zugriff: 2015-10-01.

[6] BGH: Urteil vom 10. 02. 2011 – I ZR 164/09.

Den gesetzten Cookie als Protokollierung zu verstehen ist risikoreich, da im Streitfall der Diensteanbieter das Vorliegen der Einwilligung beweisen muss.[7] Der Benutzer kann diesen Beweis – das Cookie – löschen.

Damit stellen populäre »Lösungen«, die einen kurzen Hinweis – wie die folgende Grafik beispielhaft zeigt – im Kopf einer Webseite einblenden, der über das Setzen von Cookies informiert und mit »OK« bestätigt werden soll, keine Einwilligung durch den Besucher der Webseite dar. Diesen »Lösungen« fehlt es an:

- den inhaltlichen Pflichtangaben,
- einer aussagekräftigen Protokollierung sowie
- einer bewussten und eindeutigen Einwilligung.

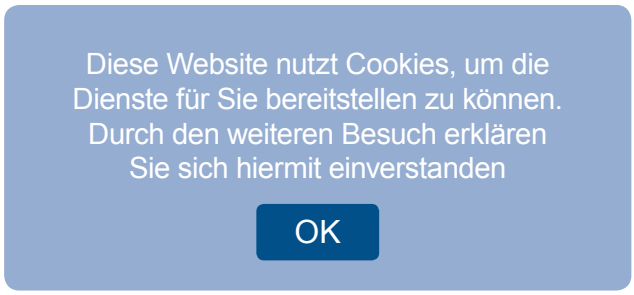


Abb. 1 *Beispiel einer beliebten »Einwilligung« zum Setzen von Cookies*

Eine Einwilligung erfordert jedoch nicht nur die bekannten Pflichtinhalte. Vielmehr muss auch die Möglichkeit bestehen, sie nicht zu erteilen. Das folgende – nicht rechtsichere – Beispiel zeigt, wie im Prinzip eine Einwilligung über die Speicherung von Tracking-Cookies aussehen könnte. Hierbei wird die Ansicht der Europäischen Kommission zugrunde gelegt, wonach weitere Informationen über die Cookies auch verlinkt werden dürfen.[8] Hierbei stellt sich jedoch die Frage, inwieweit diese Ansicht mit dem deutschen Transparenzgebot vereinbar ist.

Insbesondere bei Tracking-Cookies von Drittanbietern, wie z. B. Google Analytics, ist zu beachten, dass diese erst gesetzt werden dürfen, wenn der Benutzer auf der Webseite eingewilligt hat. Die Standardimplementation von Google Analytics prüft das Vorliegen einer Einwilligung jedoch nicht, d. h. hier besteht Anpassungsbedarf durch den Betreiber der Webseite. Google hat seine Benutzer im Sommer 2015 explizit darauf hingewiesen, dass sie Einwilligungen der Endnutzer einholen müssen und alle hierzu benötigten Informationen offen gelegt werden müssen. Die Verantwortung für das Einholen der Einwilligungen liegt weiterhin beim Webseitenbetreiber.

Eine Einwilligung gegenüber Google als Anbieter verschiedenster Dienste ist tendenziell unwirksam, da diese nicht alle betroffenen Webseiten auflisten kann und deshalb nicht hinreichend bestimmt sein wird.

Umsetzung der Widerspruchsmöglichkeit

Die Erstellung von Webstatistiken ist zulässig, solange der Nutzer dem nicht widersprochen hat (§ 15 Abs. 3 TMG). Inwieweit § 15 Abs. 3 TMG im Lichte der DS-GVO weiter Bestand haben wird, bleibt einer anderen Analyse vorbehalten.

Der Widerspruch wird in der Praxis meist durch das Anklicken eines Links oder das Setzen eines Häkchens ermöglicht. Dadurch wird dann ein Cookie auf dem Gerät des Nutzers gesetzt, der das Tracking verhindert. Diese Methode wird u. a. vom Bayerischen Landesamt für Datenschutzaufsicht anerkannt.[9]

Im Zusammenspiel mit der Cookie-Richtlinie entsteht eine widersprüchliche Situation, da das Opt-Out-Cookie in der Regel ohne eine Einwilligung einzuholen gesetzt wird. Es wäre denkbar, dass der Widerspruch gegen das Setzen von Tracking-Cookies nur zusammen mit einer gleichzeitigen Einwilligung in das Setzen des Opt-Out-Cookies erklärt werden kann. Dies würde zu der absurden Situation führen, dass im Falle des alleinigen Widerspruchs gegen die Einwilligung in das Setzen des Opt-Out-Cookies, der Webseitenbetreiber den Opt-Out-Cookie löschen müsste, aber gleichzeitig auch weiterhin keine Tracking-Cookies mehr setzen dürfte. Ohne den Opt-Out-Cookie wäre der Websei-

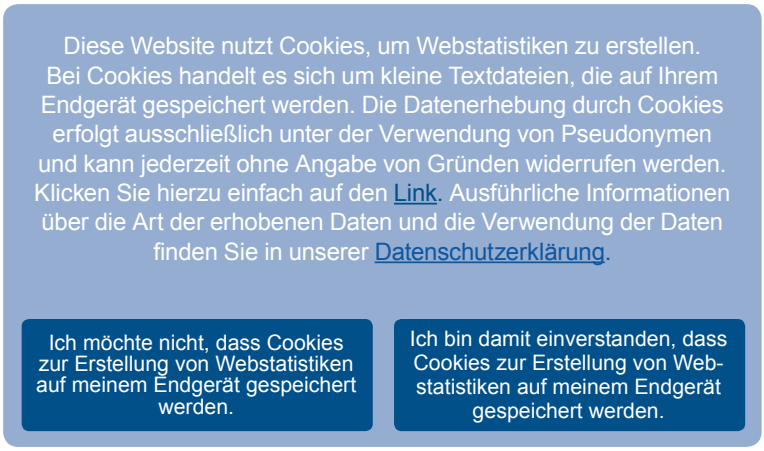


Abb. 2 *Beispiel einer datenschutzrechtlich akzeptablen Einwilligung*

[7] Taeger/Gabel-Moos (2010): § 13 TMG, Rn. 26.

[8] Europäische Kommission (2015): Cookies. URL: *http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm#section_5* Letzter Zugriff: 2015-11-26

[9] Bayerisches Landesamt für Datenschutzaufsicht (2013): Onlineprüfung Adobe Analytics (Omniture). URL: *http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm#section_5* Letzter Zugriff: 2015-11-26.

tenbetreiber aber gar nicht mehr in der Lage zu erkennen, dass auf einem Gerät keine Tracking-Cookies mehr gesetzt werden dürfen. Die Autoren freuen sich über jeden Hinweis, wie ein solcher Widerspruch rechtssicher technisch umgesetzt werden kann.

Die Cookie-Richtlinie in einzelnen Ländern

Die EU hat ihren Mitgliedsstaaten für die Umsetzung der Cookie-Richtlinie in nationales Recht eine Frist bis zum 25.05.2011 eingeräumt. Die Umsetzung und Interpretation der Richtlinie erfolgte in den verschiedenen Mitgliedsstaaten sehr unterschiedlich.[10] Eine vollständige Umsetzung fehlt in einigen Staaten bisher sogar komplett.[11]

Im Folgenden werden wir beispielhaft den Umgang mit Tracking-Cookies in Deutschland, Österreich und Großbritannien aufzeigen.

Keine Umsetzung in Deutschland?

Es ist stark umstritten, ob die Cookie-Richtlinie in Deutschland umgesetzt wurde. Es gibt keine gesetzliche Vorschrift, die dem Wortlaut der Cookie-Richtlinie entspricht oder die zu ihrer Umsetzung erlassen bzw. geändert wurde. Das TMG enthält weder das Wort Cookie noch regelt es Techniken, die der Funktionsweise von Cookies entsprechen.

Es gab einen Änderungsvorschlag zu den entsprechenden Vorschriften des TMG, welcher jedoch am 18.10.2012 vom Bundestag abgelehnt wurde.[12] Das Bundeswirtschaftsministerium vertritt dennoch die Ansicht, dass Deutschland die Cookie-Richtlinie in nationales Recht umgesetzt hat. Die europäische Kommission hat diese Ansicht gegenüber dem Portal Telemedicus bestätigt.[13] Außerdem hat Deutschland einen Fragebogen zur Umsetzung der Richtlinie ausgefüllt und dieser wurde von der Kommission nicht beanstandet. Der ausgefüllte Fragebogen wird vom zuständigen Bundeswirtschaftsministerium nicht veröffentlicht.[14]

Die Datenschutzbeauftragten des Bundes und der Länder als Aufsichtsbehörden für den Datenschutz sehen die europarechtlichen Vorgaben in Deutschland nur unvollständig umgesetzt. Sie fordern daher die Bundesregierung auf, die Richtlinie vollständig und ohne weitere Verzögerungen in nationales Recht umzusetzen. Ihrer Meinung nach muss vor dem Setzen von Cookies oder bei einem Zugriff auf diese eine Einwilligung des Nutzers eingeholt werden.[15] Diese Einschätzung wird von der Verbraucherzentrale Bundesverband (vzbv) und der Artikel-29-Gruppe[16] der Europäischen Union geteilt.[17,18] Die Bundesdatenschutzbeauftragte sagt dazu in ihrem 25. Tätigkeitsbericht:

> *»Ich empfehle dem Gesetzgeber, die Einwilligungslösung vor Setzen eines Cookies durch eine normenklare Regelung im Telemediengesetz umzusetzen.*
>
> *Wegen der teils unterschiedlichen Auslegung der Regelung hat die Artikel-29-Gruppe im Oktober 2013 ein Papier mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies […] und im November 2014 ein ergänzendes Papier zur Anwendbarkeit des Artikels 5 Absatz 3 bei Device Fingerprinting veröffentlicht […]. Beide Papiere lassen keinen Zweifel daran, dass für das Setzen von Cookies und die Berechnung eines ‚Fingerabdrucks' die Einwilligung des Nutzers erforderlich ist.«* [19]

Solange keine Novellierung der einschlägigen Vorschriften vorgenommen wird, bleiben die bisherigen in Kraft und sind grundsätzlich weiterhin anwendbar. Das TMG erlaubt die Erstellung von pseudonymen Nutzungsprofilen für Zwecke der Werbung, der Marktforschung und der bedarfsgerechten Gestaltung der Telemedien, sofern der Nutzer dem nicht widerspricht. Der Nutzer muss allerdings über sein Widerspruchsrecht informiert werden und die Zusammenführung der Nutzungsprofile mit anderen Daten über den Nutzer ist nicht gestattet (§ 15 Abs. 3 TMG). Welche Technik für die Erstellung der Nutzungsprofile eingesetzt wird, ist dabei unerheblich. Daher ist die Vorschrift auch für Tracking-Cookies einschlägig und diese können gesetzt werden, solange kein Widerspruch vorliegt. Diese Vorschrift muss jedoch konform mit der Cookie-Richtlinie ausgelegt werden, die eine Einwilligung in das Setzen von Cookies vorsieht. Es bleibt unklar, wie diese – sich widersprechenden – Vorgehensweisen in der Praxis miteinander vereint werden sollen. ▸

[10] Governor Technology Ltd (2014): About the EU Cookie Law. URL: *http://cookiepedia.co.uk/cookie-laws-across-europe* Letzter Zugriff: 2015-10-02.

[11] Computerwoche (2015): »Cookie-Richtlinie« in Europa. URL: *http://www.computerwoche.de/a/cookie-richtlinie-in-europa,2518064* Letzter Zugriff: 2015-10-02.

[12] Deutscher Bundestag (2012): Die Beschlüsse des Bundestages am 18. Oktober. URL: *http://www.bundestag.de/dokumente/textarchiv/2012/41022790_kw42_angenommen_abgelehnt/209690* Letzter Zugriff: 2015-10-02.

[13] Telemedicus e.V. (2014): EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt. URL: *http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html* Letzter Zugriff: 2015-11-13.

[14] Telemedicus e.V. (2014): EU-Kommission: Cookie-Richtlinie ist in Deutschland umgesetzt. URL: *http://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html* Letzter Zugriff: 2015-11-13.

[15] Umlaufentschließung der Datenschutzbeauftragten des Bundes und der Länder vom 05. Februar 2015 (2015): Keine Cookies ohne Einwilligung der Internetnutzer. URL: *http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/Entschliessung_Cookies.pdf?__blob=publicationFile&v=9* Letzter Zugriff: 2015-10-01.

[16] Artikel-29-Gruppe: »Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie. […] Eine wesentliche Aufgabe der Gruppe neben der Beratung der Kommission ist es, die Harmonisierung des Datenschutzes innerhalb der Europäischen Union voranzutreiben. Die Gruppe trifft sich in der Regel fünf Mal pro Jahr in Brüssel zu zweitägigen Sitzungen und wird in ihrer Arbeit durch Untergruppen unterstützt. In den letzten Jahren waren Untergruppen zu den Themenbereichen Internet, Passagierdaten und verbindlichen Unternehmensrichtlinien aktiv.« Quelle: BfDI. URL: *http://www.bfdi.bund.de/DE/Europa_International/Europa/Ueberblick/DatenschutzgruppeArt29EG.html?nn=5217120* Letzter Zugriff: 2015-12-06.

[17] Verbraucherzentrale Bundesverband (2015): Cookies nur mit Einwilligung. URL: *http://www.vzbv.de/meldung/cookies-nur-mit-einwilligung*. Letzter Zugriff: 2015-10-02.

[18] Article 29 Data Protection Working Party (2013): Working Document 02/2013 providing guidance on obtaining consent for cookies (WP 208 vom 2.10.2013). URL: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf* Letzter Zugriff: 2015-12-06.

[19] Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (2015): Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014, S. 159.

Unsere Untersuchung der 10 meistbesuchten Webseiten in Deutschland[20] im Juli 2015 hat ergeben, dass die rechtlichen Vorgaben nicht einheitlich umgesetzt werden. Keine der besuchten Webseiten hat eine ausdrückliche Einwilligung in die Nutzung von Cookies verlangt. Stattdessen gehen vier der besuchten Webseiten von einer Einwilligung durch die Browsereinstellungen aus. Sechs Webseiten setzen gleichzeitig auf Einwilligungen durch die Browsereinstellungen und konkludente Einwilligungen durch den Besuch der Webseite. Aus juristischer Sicht sind zwei Einwilligungen für denselben Sachverhalt nicht nur nicht notwendig sondern werfen auch die Frage auf, ob dieses Vorgehen alleine wegen fehlender Eindeutigkeit zur Nichtigkeit der Einwilligung führt.

Eine konkludente Einwilligung widerspricht zudem der Anforderung, dass eine elektronische Einwilligung vor dem Rechtsgeschäft, also hier dem Setzen von Tracking-Cookies, eingeholt werden muss und der Nutzer dabei eine bewusste und eindeutige Einwilligung erteilt hat sowie auf sein Widerrufsrecht hingewiesen worden ist (§ 13 Abs. 2, 3 TMG). Diese Voraussetzungen sind nicht erfüllt, wenn der Nutzer erst selber auf der Webseite nach Informationen über Cookies suchen muss jedoch beim ersten Seitenaufruf Tracking-Cookies gesetzt werden. Zudem kann die vermeintliche Einwilligung nicht protokolliert werden (§ 13 Abs. 2 Nr. 2 TMG) (vgl. 2).

Auch eine Einwilligung durch die eigenen Browsereinstellungen erfüllt die gesetzlichen Anforderungen nicht, da sie weder protokolliert werden kann noch sicherstellt, dass der Nutzer die Einwilligung bezogen auf die jeweilige Webseite bewusst und eindeutig erteilt hat. Letzteres ist nicht gegeben, da nicht alle Browser notwendigerweise Informationen über Cookies und die Möglichkeit diese zu verwalten anbieten. Insbesondere die Differenzierung nach unterschiedlichen Webseiten ist nicht bei jedem Browser möglich. Zudem ist eine Nutzung des Browser meist möglich, ohne vorher die Einstellungen über Cookies anzupassen. Aus diesen Gründen ist dringend davon abzuraten, die Browsereinstellungen als Einwilligung für das Setzen von Cookies zu verstehen.

Rechtsunsicherheit in Österreich

In Österreich erfolgte die Umsetzung der Cookie-Richtlinie in § 96 Abs. 3 TKG (österr. Telekommunikationsgesetz). Die Änderung ist am 22.11.2011 und damit knapp ein halbes Jahr nach dem Ende der Umsetzungsfrist in Kraft getreten.

Die Betreiber von öffentlichen Telekommunikationsdiensten und Diensteanbieter müssen Teilnehmer und Benutzer bei der Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten über den Zweck, die zugrunde liegende Rechtsgrundlage und darüber, wie lange die Daten gespeichert werden, informieren. Eine Ermittlung der Daten ist nur mit Einwilligung des Betroffenen möglich (§ 96 Abs. 3 S. 1 und 2 österr. TKG). Von dieser Vorschrift sind Tracking-Cookies betroffen, da sie personenbezogene Daten ermitteln, verarbeiten und übermitteln können. Besondere Anforderungen, die von denen des österr. Datenschutzgesetzes an die Einwilligung (im Wortlaut »Zustimmung«) abweichen, nennt das österr. TKG nicht.

Die Einwilligung ist entbehrlich, wenn die Speicherung ausschließlich erfolgt, um eine Nachricht zu übertragen oder sie für die Nutzung eines Dienstes erforderlich ist, den der Betroffene angefordert hat (§ 96 Abs. 3 S. 3 österr. TKG). Daher muss für Session-Cookies auch in Österreich keine Einwilligung eingeholt werden.

Die Wirtschaftskammer Österreich vertritt die Ansicht, dass die Einwilligung zum Setzen von Cookies auch konkludent über die Browsereinstellungen erfolgen kann. Der Informationspflicht könne durch eine Datenschutzerklärung genüge getan werden.[21] Private Stellen schließen sich dieser Ansicht an.[22,23] Dennoch scheint es an Rechtssicherheit zu fehlen, da sich weder die Österreichische Datenschutzbehörde (DSB) zu diesem Thema geäußert hat, noch höchstrichterliche Rechtsprechung den Autoren zu dieser Frage bekannt ist.

Wer nicht über das Setzen von Tracking-Cookies informiert, dem droht ein Bußgeld in Höhe von bis zu 37.000 € (§ 109 Abs. 3 österr. TKG). Eine nicht eingeholte Einwilligung scheint nicht bußgeldbewährt zu sein. Daher ist es wenig verwunderlich, dass österreichische Webseitenbetreiber auf die Einholung einer ausdrücklichen Einwilligung verzichten und den Besucher lediglich in

[20] Gemäß der Auswertung von *Alexa.com*, wobei dem Ranking eine Kombination des Durchschnitts der täglichen Besucher und der Zahl der Seitenaufrufe der letzten Monate zugrunde liegen.

[21] Wirtschaftskammer Österreich (2015): Was ist im Zusammenhang mit Werbung, Online-Werbung und Datenschutz zu beachten? URL: *https://www.wko.at/Content.Node/branchen/oe/sparte_iuc/Werbung-und-Marktkommunikation/Was_ist_im_Zusammenhang_mit_Werbung,_Online-Werbung_und_Da.html*
Letzter Zugriff: 2015-10-02.

[22] artworx gmbh (2015): Die »Cookie Richtlinie« der EU: In Österreich ist Opt-In für personenbezogene Daten Gesetz. URL: *http://www.artworx.at/die-cookie-richtlinie-der-eu-in-oesterreich-ist-opt-in-fuer-personenbezogene-daten-gesetz*
Letzter Zugriff: 2015-10-02.

[23] Dr. Schweiger & Partner Rechtsanwälte OG (2012): Umsetzung der Cookie-Richtlinie im TelekommunikationsG. URL: *http://www.it-recht.at/index.php/aktuelles/246-umsetzung-der-cookie-richtlinie-im-telekommunikationsg*
Letzter Zugriff: 2015-10-02.

der Datenschutzerklärung über die Cookies informieren, wie wir in unserer Untersuchung der 10 meistbesuchten Webseiten in Österreich[24] im Juli 2015 festgestellt haben.

Keine der besuchten Webseiten hat eine ausdrückliche Einwilligung für Cookies eingeholt. Vier der besuchten Webseiten gingen von einer Einwilligung durch die eigenen Browsereinstellungen aus. Sechs Webseiten setzen hingegen gleichzeitig auf Einwilligungen durch die Browsereinstellungen und konkludente Einwilligungen durch den Besuch der Webseite. Der Informationspflicht sind alle besuchten Webseiten nachgekommen, auch wenn sie unterschiedlich umgesetzt wird. Die Varianten reichen von leicht zu findenden und ausführlichen Informationen bis zu versteckten und wenig aussagekräftigen Hinweisen.

Konkludente Einwilligung in Großbritannien

In Großbritannien wurde aufgrund der Cookie-Richtlinie das Gesetz PECR (The Privacy and Electronic Communications (EC Directive) Regulations 2003) geändert. Das neue Gesetz trat am 26.05.2011 und damit einen Tag nach dem Ende der Umsetzungsfrist in Kraft.

Das PECR sieht vor, dass grundsätzlich keine Daten auf Endgeräten von Nutzern gespeichert werden dürfen und kein Zugang zu diesen gespeicherten Daten gewährt werden darf, wenn bestimmte Voraussetzungen nicht erfüllt sind. Für die Zulässigkeit muss der Nutzer über den Zweck der Speicherung bzw. der Zugangsgewährung umfassend und eindeutig informiert worden sein sowie seine Einwilligung erteilt haben (6.-(1) + (2) PECR). Demnach muss in Großbritannien für die Verwendung von Tracking-Cookies die Einwilligung des Nutzers eingeholt werden.

Diese Vorschriften greifen nicht, wenn die Daten ausschließlich für die Übertragung der Kommunikation genutzt werden, wie z. B. für den Versand von Nachrichten. Gleiches gilt, wenn die Datenspeicherung bzw. die Zugangsgewährung für die Bereitstellung eines Dienstes, den der Nutzer angefordert hat, wie z. B. die Speicherung des Inhaltes eines Warenkorbes in einem Online-Shop, erforderlich ist (6.-(4) PECR). Somit muss auch in Großbritannien keine Einwilligung eingeholt werden, wenn Session-Cookies verwendet werden.

Werden Daten bei mehr als einer Gelegenheit gespeichert bzw. Zugang zu ihnen gewährt, so ist es ausreichend, wenn die Information und Einwilligung bei der ersten Nutzung erteilt wird (6.-(3) PECR). So kann davon abgesehen werden, wiederkehrende Besucher bei jedem Besuch einer Webseite erneut um ihre Einwilligung zu bitten. Diese Erleichterung setzt im Prinzip technisch die Identifikation des Besuchers voraus. Durch Setzen eines entsprechenden Cookies kann die Einwilligung auf dem verwendeten Endgerät gespeichert werden. Nicht erteilte Einwilligungen lassen sich indes nicht durch ein Cookie »speichern«. Die naheliegende Lösung ist, den Besucher bei jedem Besuch zu fragen mit der Konsequenz, dass nur eine erteilte Einwilligung vor zukünftigen Fragen schützt.

Bei Zuwiderhandlungen gegen die genannten Vorschriften drohen Geldstrafen in Höhe bis zu 500.000 £[25], was ca. 710.000 € entspricht.

Die britische Datenschutzbehörde, The Information Commissioner, vertritt die Auffassung, dass die Einwilligung auch konkludent erteilt werden kann.[26] Hiernach kann bereits der bloße Besuch einer Webseite eine Einwilligung darstellen, solange der Nutzer aufgrund der deutlich sichtbaren Informationen versteht, dass er sich durch den weiteren Besuch der Webseite mit den Tracking-Cookies einverstanden erklärt.[27] Werden Tracking-Cookies bereits auf der ersten besuchten Seite gesetzt, bleiben diese auch beim Abbruch des Besuchs, d. h. bei einer nicht erteilten konkludenten Einwilligung regelmäßig gespeichert. Welche Webseite ein Besucher zuerst sieht, lässt sich i. d. R. nicht durch den Betreiber beeinflussen.

Unsere Untersuchung der 10 meistbesuchten Webseiten in Großbritannie[28] im Juli 2015 hat ergeben, dass diese Ansicht von britischen Webseitenbetreibern aufgegriffen wurde. Eine ausdrückliche Einwilligung wurde bei keiner der besuchten Webseiten eingeholt. Dafür fanden sich in den Datenschutzerklärungen und vergleichbaren Texten meist ausführliche Informationen über Cookies. Bei acht der besuchten Webseiten wurde gleichzeitig von einer Einwilligung durch den Besuch der Webseite und durch

[24] Gemäß der Auswertung von Alexa.com, wobei dem Ranking eine Kombination des Durchschnitts der täglichen Besucher und der Zahl der Seitenaufrufe der letzten Monate zugrunde liegen.

[25] Information Commissioner's Office: What are PECR? URL: *https://ico.org.uk/for-organisations/guide-to-pecr/introduction/what-are-pecr*
Letzter Zugriff: 2015-10-02.

[26] Information Commissioner's Office (2015): Cookies and similar technologies. URL: *https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies*
Letzter Zugriff: 2015-10-02.

[27] Information Commissioner's Office (2012): Guidance on the rules on use of cookies and similar technologies. URL: *https://ico.org.uk/media/1545/cookies_guidance.pdf*
S. 8. Letzter Zugriff: 2015-10-02.

[28] Gemäß der Auswertung von Alexa.com, wobei dem Ranking eine Kombination des Durchschnitts der täglichen Besucher und der Zahl der Seitenaufrufe der letzten Monate zugrunde liegen.

die eigenen Browsereinstellungen ausgegangen. Nur eine der besuchten Webseiten setzte ausschließlich auf eine Einwilligung durch die eigenen Browsereinstellungen und nicht zusätzlich auch auf den Besuch der Webseite an sich. Die geforderten Hinweise über Cookies sind nicht immer farblich hervorgehoben oder so groß, dass sie sofort ins Auge springen. Daher besteht die Gefahr, dass sie vom Nutzer gar nicht oder erst spät wahrgenommen werden. Positiv hervorzuheben ist eine Webseite, die zwar von einer konkludenten Einwilligung durch den Webseitenbesuch ausging, aber in einem deutlich sichtbaren Hinweis ausführlich über Cookies informierte. In den Cookie-Einstellungen konnten dann Komfort- und Tracking-Cookies mit jeweils einem Klick unabhängig voneinander deaktiviert werden.

Alternativen zur Nutzung von Cookies

Die Rechtsunsicherheit und vor allem die fehlende Praktikabilität der Anforderungen an die Verwendung von Tracking-Cookies machen daher alternative Möglichkeiten der Erstellung von Webstatistiken attraktiv. Eine solche Möglichkeit ist das sogenannte Browser Fingerprinting. Hierbei werden zusätzlich zu den im HTTP übermittelten Daten, wie z. B. Browserversion und Betriebssystem, durch den Einsatz von Scripten noch weitere Daten, wie etwa installierte Plugins, die Bildschirmauflösung oder Spracheinstellungen erhoben. Durch Kombination der einzelnen Daten kann dann ein »Fingerabdruck« entstehen, durch den ein Gerät identifiziert werden kann. Die Identifikation ist nicht zwingend eindeutig, da verschiedene Menschen die gleiche Konfiguration verwenden können. Je mehr Daten verwendet werden, desto eindeutiger wird der Fingerabdruck.

Die Artikel-29-Gruppe weist darauf hin, dass Fingerprinting, bei dem Daten von einem Endgerät ausgelesen werden, ebenfalls einer Einwilligung bedarf (vgl. 4.1).29 Auch ohne Berechnung eines Fingerprints erheben moderne Webstatistikprogramme Daten wie z. B. Bildschirmauflösung oder installierte Plugins des Endgerätes.

Wenn zusätzlich zu diesem Fingerabdruck auch noch weitere Daten, wie etwa die E-Mail-Adresse oder Anmeldeinformationen eines Online-Shops, vorhanden sind, kann es sogar möglich sein, den Nutzer namentlich zu benennen.

Eine andere Form des Fingerprintings ist das sogenannte »Canvas Fingerprinting«. Hierfür wird Canvas genutzt, ein Verfahren mit dem in javascript gezeichnet wird. Eine Vielzahl von einzelnen Canvas-Elementen kann durch Befehle von javascript zu einer Pixelgrafik angeordnet werden. Werden diese Elemente schnell gewechselt, entstehen Animationen, die vor allem für Browserspiele genutzt werden. Die Darstellung der Canvas-Elemente variiert je nach Betriebssystem, Browser, Grafikkarte und Grafiktreiber. Um einen persönlichen Fingerabdruck zu erstellen, wird dem Browser ein verstecktes Element übermittelt. Durch die individuell verschiedenen Darstellungen können ab diesem Zeitpunkt 89 % der Nutzer wiedererkannt werden.[30]

Auf eine weitere Idee zur Erstellung von Webstatistiken kam Verizon, ein großer US-amerikanischer Mobilfunkanbieter. Verizon fügt bei jedem Webseitenaufruf seiner Kunden dem Header der aufgerufenen Webseite eine individuelle Zeichenkombination hinzu. So kann eindeutig nachvollzogen werden, welche Webseiten von welchem Nutzer besucht wurden. Die so erlangten Webstatistiken werden an Werbetreibende verkauft.

Werden Webstatistiken mittels Fingerprinting erstellt oder findet eine heimliche Überwachung wie bei Verizon statt, merkt der Nutzer davon in der Regel nichts. Eine Analyse des Quellcodes dürfte durchschnittliche Besucher überfordern. Insbesondere dann, wenn die Verständlichkeit des Quellcodes gezielt durch Verschleierungstechniken erschwert wird. Wofür erhobene Daten verwendet werden, verrät der Webseitenquellcode indes nicht. Selbst wenn der Nutzer den Verdacht hegt, überwacht zu werden, kann er es technisch nicht ohne weiteres verhindern. Auch die Erstattung einer Anzeige erscheint mangels Beweisen nur wenig erfolgsversprechend.

Cookies hingegen bieten für den Nutzer den Vorteil, dass sie durch die Browsereinstellungen jederzeit gelöscht oder blockiert werden können, sodass Webstatistiken nicht (mehr) erstellt werden können. Zudem sind die Cookies und

[29] Artikel 29 Data Protection Working Party (2014): Opinion 9/2014 on the application of Directive 2002/58/EC to device fingerprinting. URL: *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf*. Letzter Zugriff 2015-12-07.

[30] Heise Medien GmbH & Co. KG (2014): Fingerabdrücke auf der Leinwand - Browserprofile mit Canvas-Fingerprinting. URL: *http://www.heise.de/ct/ausgabe/2014-18-Browserprofile-mit-Canvas-Fingerprinting-2283693.html*. Letzter Zugriff: 2015-11-13.

[31] Heise Medien GmbH & Co. KG (2014): Supercookie: US-Provider Verizon verkauft Daten über seine Kunden. URL: *http://www.heise.de/security/meldung/Supercookie-US-Provider-Verizon-verkauft-Daten-ueber-seine-Kunden-2437242.html*. Letzter Zugriff: 2015-11-04.

die Webseite, die sie gesetzt hat, im Browser einzeln zu sehen. Dadurch kann der Nutzer erfahren, wenn er Teil einer Webstatistik geworden ist und Verstöße ggf. zur Anzeige bringen.

Fazit

Wie wir gesehen haben, wurde die Cookie-Richtlinie innerhalb der EU bisher nicht einheitlich umgesetzt. In einigen Ländern fehlt die Umsetzung bis heute sogar komplett und die jeweiligen nationalen Gesetzgebungen müssen im Sinne der Cookie-Richtlinie ausgelegt werden. Eine eindeutige Antwort auf die Frage, wie dies in der Praxis aussehen soll, insbesondere bei offensichtlichen Widersprüchen zur Cookie-Richtlinie und zum nationalen Recht, gibt es nicht. Daher bestehen in diesen Ländern große Unsicherheiten darüber, unter welchen Voraussetzungen Tracking-Cookies gesetzt werden dürfen. Dies macht die Nutzung alternativer Methoden zur Erstellung von Webstatistiken, wie etwa Fingerprinting, für Webseitenbetreiber umso attraktiver. Für den Nutzer haben alternative Methoden gegenüber dem Einsatz von Cookies jedoch den Nachteil, dass er in der Regel die Erstellung von Webstatistiken nicht verhindern kann und meist auch gar nicht weiß, dass er Teil einer solchen ist.

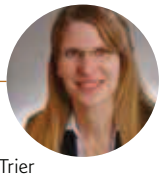
Aufgrund der uneinheitlichen Umsetzung der Cookie-Richtlinie gelten innerhalb der EU nun unterschiedliche Vorschriften für Tracking-Cookies. Was in einem Land erlaubt ist oder toleriert wird, kann in einem anderen Land verboten und mit hohen Geldbußen belegt sein. Dies stellt insbesondere für multinationale Unternehmen eine große Herausforderung dar. Soll eine Webseite in verschiedenen Ländern zur Verfügung stehen, ist es nicht ausreichend, sie in die jeweiligen Landessprachen zu übersetzen. Vielmehr muss der Einsatz von Cookies für jedes Land separat bewertet und dann entsprechend umgesetzt werden. Das Ziel eines einheitlichen Rechts innerhalb der Europäischen Union wurde hier klar verfehlt.

Eine Änderung der Cookie-Richtlinie wird durch die DS-GVO gefordert, um diese an die Regeln der DS-GVO anzupassen (vgl. Erwägungsgrund 135 DS-GVO). Es bleibt daher abzuwarten, wie sich die Rechtslage zukünftig entwickeln wird.

Es gibt heute keine überzeugende technische Möglichkeit, um die Cookie-Richtlinie in der Praxis umzusetzen. Es müsste möglich sein, dass erst nach erteilter Einwilligung mit der Erstellung von Webstatistiken begonnen wird. Für die Wirksamkeit der Einwilligung müssten die umfangreichen Informationspflichten erfüllt werden, die immer die Gefahr bergen, intransparent und damit nichtig zu sein. Das bedeutet, dass keine Tracking-Cookies gesetzt und Informationen aus dem Endgerät ausgelesen werden dürfen, solange (noch) keine wirksame Einwilligung vorliegt. Vorliegende Einwilligungen müssten protokolliert und der Nutzer identifiziert werden, damit auch nachvollziehbar ist, welcher Nutzer seine Einwilligung erteilt hat. Es besteht Grund zu der Annahme, dass viele Webseitenbesucher ihre Einwilligung nicht erteilen würden, wenn diese ausdrücklich von ihnen verlangt werden würde.

In Anbetracht dieser Tatsachen scheint die Cookie Richtlinie mehr Schaden anzurichten als Nutzen zu stiften.

Über die Autoren



Mareike Papendorf
Mareike Papendorf hat Wirtschaftsrecht an den Hochschulen Köln und Trier studiert. Sie ist bei der Xamit Bewertungsgesellschaft mbH als Beraterin beschäftigt. Ihr Tätigkeitsschwerpunkt liegt auf dem Datenschutzrecht.

Niels Lepperhoff
Niels Lepperhoff ist Geschäftsführer der Xamit Bewertungsgesellschaft mbH und der DSZ Datenschutz Zertifizierungsgesellschaft mbH (dem Gemeinschaftsunternehmen des BvD und der GDD). Er verfügt über langjährige Berufserfahrung als externer Datenschutzbeauftragter und berät sowohl deutsche als auch internationale Unternehmen.

▶ www.xamit-leistungen.de

XAMIT