



00879/12/DE
WP 194

**Stellungnahme 04/2012 zur Ausnahme von Cookies von der
Einwilligungspflicht**

Angenommen am 7. Juni 2012

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Direktion C (Grundrechte und Unionsbürgerschaft), der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro MO59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_de.htm

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung,

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1 Einleitung

Artikel 5 Absatz 3 der Richtlinie 2002/58/EG, geändert durch Richtlinie 2009/136/EG, sieht für die Speicherung von Informationen oder den Zugriff auf Informationen auf dem Endgerät des Nutzers (oder Teilnehmers) eine Einwilligung in Kenntnis der Sachlage vor und stärkt damit den Schutz der Nutzer elektronischer Kommunikationsnetze und -dienste. Dieses Erfordernis gilt für alle Arten von Informationen, die auf dem Endgerät des Nutzers gespeichert werden oder auf die dort zugegriffen wird, wenngleich die Diskussionen im Wesentlichen die Verwendung von Cookies im Sinne der Definition in RFC 6265¹ betreffen. Deshalb wird in dieser Stellungnahme erläutert, wie sich die Neufassung von Artikel 5 Absatz 3 auf die Verwendung von Cookies auswirkt, wobei der Begriff vergleichbare Technologien nicht ausschließt.

Nach Artikel 5 Absatz 3 ist für Cookies keine Einwilligung in Kenntnis der Sachlage erforderlich, wenn sie einem der folgenden Kriterien entsprechen:

Kriterium A: Der Cookie wird verwendet, *„wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist“*.

Kriterium B: Der Cookie wird verwendet, *„wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann“*.

Nachdem die Datenschutzgruppe die Anforderungen an die Einwilligung in Kenntnis der Sachlage bereits in zwei Stellungnahmen² eingehend untersucht hat, sind die für Cookies und vergleichbare Technologien geltenden Ausnahmen von diesem Grundsatz Gegenstand der vorliegenden Stellungnahme.

Diese Analyse berührt weder das Recht auf Unterrichtung noch das letztendliche Widerspruchsrecht nach der Richtlinie 95/46/EG, die beide für die Verarbeitung personenbezogener Daten unabhängig davon gelten, ob Cookies verwendet werden oder nicht.

¹ <http://tools.ietf.org/html/rfc6265>

² Stellungnahme 2/2010 zur „Werbung auf Basis von Behavioural Targeting“ und Stellungnahme 16/2011 zur „Best-Practice-Empfehlung von EASA und IAB zu verhaltensorientierter Online-Werbung“.

2 Analyse

2.1 Kriterium A

Die Formulierung „der alleinige Zweck“ in Kriterium A schränkt die unter Verwendung von Cookies zulässigen Arten der Verarbeitung ausdrücklich ein und lässt wenig Auslegungsspielraum. Ein Cookie darf nicht ohne weiteres verwendet werden, um die Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz zu beschleunigen oder zu regulieren. Vielmehr muss die Übertragung der Nachricht ohne Verwendung des Cookies unmöglich sein. Es ist anzumerken, dass die ursprüngliche Fassung der Richtlinie 2002/58/EG Artikel 5 Absatz 3 bereits diese Ausnahme für Cookies enthielt, die verwendet werden durften *„wenn der alleinige Zweck die Durchführung oder Erleichterung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz“* war. In der überarbeiteten Richtlinie wurde derselbe Wortlaut verwendet, jedoch unter Streichung der Worte *„oder Erleichterung“*, was als weiteres Indiz dafür ausgelegt werden kann, dass der europäische Gesetzgeber beabsichtigte, den Umfang der in Artikel 5 Absatz 3 nach Kriterium A gewährten Ausnahme einzuschränken.

Für die Übertragung von Nachrichten zwischen zwei Parteien über ein Netz sind mindestens drei Elemente als unbedingt notwendig anzusehen:

- 1) die Fähigkeit, die Informationen über das Netz weiterzuleiten, insbesondere durch Erkennung der Verbindungsendpunkte,
- 2) die Fähigkeit, Datenelemente in den vorgesehenen Reihenfolge auszutauschen, insbesondere durch die Nummerierung von Datenpaketen,
- 3) die Fähigkeit, Übertragungsfehler oder Datenverlust zu erkennen.

Die Formulierung *„Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz“* in Kriterium A – und insbesondere das Wort *„über“* – bezieht sich auf jedwede Art des Datenaustauschs mithilfe eines elektronischen Kommunikationsnetzes (im Sinne der Richtlinie 2002/21/EG) und schließt damit potenziell auch den Datenaustausch auf „Anwendungsebene“ ohne Beschränkung auf den zur Bildung des elektronischen Kommunikationsnetzes erforderlichen Austausch technischer Daten ein, wenn dieser zumindest eine der oben definierten Eigenschaften aufweist.

Insofern umfasst das Kriterium A auch Cookies, die mindestens eine der oben definierten Eigenschaften für Übertragungen über das Internet aufweisen.

2.2 Kriterium B

In ähnlicher Weise deutet der Wortlaut von Kriterium B darauf hin, dass der europäische Gesetzgeber die hohen Hürden für die Inanspruchnahme der Ausnahmeregelung aufrechterhalten wollte. Nach unmittelbarer Interpretation der Richtlinie muss ein Cookie, um Kriterium B zu entsprechen, gleichzeitig die beiden folgenden Voraussetzungen erfüllen:

- 1) Der Dienst der Informationsgesellschaft wurde vom Nutzer ausdrücklich gewünscht: Der Nutzer (oder Teilnehmer) hat selbst etwas unternommen, um einen Dienst mit einem klar definierten Umfang anzufordern.

- 2) Der Cookie ist für den Dienst der Informationsgesellschaft unbedingt erforderlich:
Wenn Cookies deaktiviert sind, funktioniert der Dienst nicht.

Darüber hinaus wird in Erwägungsgrund 66 der Richtlinie 2009/136/EG betont: „*Ausnahmen von der Informationspflicht und der Einräumung des Rechts auf Ablehnung sollten auf jene Situationen beschränkt sein, in denen die technische Speicherung oder der Zugriff unverzichtbar sind, um die Nutzung eines vom Teilnehmer oder Nutzer ausdrücklich angeforderten Dienstes zu ermöglichen.*“ Damit die Ausnahmeregelung greift, muss kurzum ein klarer Zusammenhang zwischen der unbedingten Notwendigkeit eines Cookies und dem vom Nutzer ausdrücklich angeforderten Dienst bestehen.

Selbst bei dieser Interpretation der Richtlinie bleibt zu klären, welchen Umfang ein Dienst „*der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde*“, hat. Ein Dienst der Informationsgesellschaft kann sich aus vielen Komponenten zusammensetzen, von denen einige nicht von allen Nutzern verwendet oder nur für den Bedarfsfall zur Verfügung gestellt werden. So kann etwa eine Online-Zeitung für jedermann frei zugänglich sein, jedoch für angemeldete Nutzer zusätzliche Funktionen bieten, beispielsweise die Möglichkeit, Kommentare zu Artikeln zu hinterlassen. Diese zusätzlichen Funktionen können wiederum durch eigene Cookies ermöglicht werden. In diesem speziellen Zusammenhang ist ein Dienst der Informationsgesellschaft nach Ansicht der Datenschutzgruppe als die Summe verschiedener Funktionen zu betrachten und kann deshalb je nach den vom Nutzer (oder Teilnehmer) angeforderten Funktionen einen unterschiedlichen Umfang aufweisen.

Kriterium B lässt sich somit auch anhand der von einem Dienst der Informationsgesellschaft zur Verfügung gestellten Funktionen definieren. In diesem Sinne müssten Cookies, um Kriterium B zu entsprechen, folgende Voraussetzungen erfüllen:

- 1) Ein Cookie ist erforderlich, um dem Nutzer (oder Teilnehmer) eine bestimmte Funktion zur Verfügung zu stellen: Wenn Cookies deaktiviert sind, ist die Funktion nicht verfügbar.
- 2) Die Funktion wurde vom Nutzer (oder Teilnehmer) als Teil eines Dienstes der Informationsgesellschaft ausdrücklich angefordert.

2.3 Merkmale eines Cookies

Cookies werden häufig nach folgenden Merkmalen unterschieden:

- 1) ob es sich um „Sitzungscookies“ oder „persistente Cookies“ handelt
- 2) ob es sich um Cookies von Drittanbietern, sogenannte „Third-Party-Cookies“, handelt oder nicht

Ein „Sitzungscookie“ ist ein Cookie, der automatisch gelöscht wird, wenn der Nutzer seinen Browser schließt, während ein „persistenter Cookie“ ein Cookie ist, der auf dem Endgerät des Nutzers bis zu einem festgelegten Ablaufdatum (das Minuten, Tage oder auch mehrere Jahre in der Zukunft liegen kann) gespeichert bleibt.

Der Begriff „Third-Party-Cookie“ kann irreführend sein:

- Im Kontext der europäischen Datenschutzvorschriften definiert die Richtlinie 95/46/EG einen Dritten (englisch: „third party“) als *„natürliche oder juristische Person, Behörde, Einrichtung oder jede andere Stelle, außer der betroffenen Person, dem für die Verarbeitung Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters befugt sind, die Daten zu verarbeiten“*. Ein „Third-Party-Cookie“ wäre demnach ein Cookie, der von einem für die Verarbeitung Verantwortlichen gesetzt wurde, der nicht mit dem Betreiber der vom Nutzer besuchten Website (definiert durch die in der Adresszeile des Browsers angezeigte URL) identisch ist.
- Aus Browsersicht wird der Begriff „Third Party“ jedoch ausschließlich durch die Struktur der in der Adresszeile des Browsers angezeigten URL bestimmt. In diesem Fall sind „Third-Party-Cookies“ solche, die von Websites gesetzt werden, deren Domäne nicht mit der Domäne der vom Nutzer besuchten und in der Adresszeile des Browsers angezeigten Website übereinstimmt, unabhängig davon, ob es sich um unterschiedliche für die Verarbeitung Verantwortliche handelt oder nicht.

Diese beiden Konzepte überschneiden sich zwar häufig, sind aber nicht immer identisch. Für diese Stellungnahme folgen wir dem ersten Konzept und verwenden den Begriff „Third-Party-Cookie“ für Cookies, die von für die Verarbeitung Verantwortlichen gesetzt werden, die nicht mit dem Betreiber der vom Nutzer gerade besuchten Website identisch sind. Umgekehrt bezeichnet der Begriff „First-Party-Cookie“ einen Cookie, der von einem für die Verarbeitung Verantwortlichen (oder einem seiner Auftragsverarbeiter) gesetzt wird, der die vom Nutzer besuchte und an der in der Adresszeile des Browsers angezeigten URL erkennbare Website betreibt.

Um zu beurteilen, ob ein Cookie gemäß den Formulierungen in den Kriterien A bzw. B für einen Dienst *„unbedingt erforderlich“*, vom *„Nutzer ausdrücklich gewünscht“* oder auf einen *„alleinige[n] Zweck“* beschränkt ist, werden bestimmte Merkmale herangezogen.

Die Gültigkeitsdauer eines von der Einwilligungspflicht ausgenommenen Cookies sollte in unmittelbarem Zusammenhang mit seinem Verwendungszweck stehen und muss unter Berücksichtigung der berechtigten Erwartungen des durchschnittlichen Nutzers oder Teilnehmers so bemessen sein, dass der Cookie abläuft, sobald er nicht mehr erforderlich ist. Dies legt nahe, dass Cookies, die den Kriterien A und B entsprechen, wahrscheinlich mit dem Ende der Browsersitzung, wenn nicht sogar früher ablaufen. Dies ist jedoch nicht immer der Fall. So könnte etwa in dem im folgenden Abschnitt dargelegten Anwendungsfall des Warenkorbs ein Händler den Cookie so setzen, dass er über das Ende der Browsersitzung hinaus oder einige Stunden lang gültig bleibt, weil der Nutzer seinen Browser versehentlich schließen und dann berechtigterweise erwarten könnte, den Inhalt seines Warenkorbs noch vorzufinden, wenn er in den folgenden Minuten auf die Website des Händlers zurückkehrt. In anderen Fällen kann es der ausdrückliche Wunsch des Nutzers sein, dass der Dienst bestimmte Informationen bis zur nächsten Sitzung speichert, was die Verwendung eines persistenten Cookies erfordert.

Ferner sind Third-Party-Cookies im Sinne der obigen Definitionen für den Nutzer, der eine Website besucht, in der Regel nicht „*unbedingt erforderlich*“, weil sie gewöhnlich mit einem Dienst im Zusammenhang stehen, der sich von dem vom Nutzer *ausdrücklich gewünschten* Dienst unterscheidet.

Daher sind First-Party-Sitzungscookies mit wesentlich höherer Wahrscheinlichkeit von der Einwilligungspflicht ausgenommen als persistente Third-Party-Cookies³. Doch wenngleich diese Merkmale erste Anhaltspunkte für die Priorisierung von Konformitätsmaßnahmen bieten können, reichen sie allein nicht aus, um festzustellen, ob ein Cookie den Kriterien A oder B entspricht. Man stelle sich einen Cookie vor, der verwendet wird, um Nutzer, die sich auf einer Website einloggen, zu authentifizieren. Dieser Cookie soll gewährleisten, dass der Nutzer nur auf Inhalte zugreifen kann, für die er eine Zugriffsberechtigung besitzt. Ein ähnlicher Cookie kann verwendet werden, um Nutzer auf einer Domäne zu identifizieren und zu verfolgen und ihnen anhand des vom Betreiber der Website angelegten Profils maßgeschneiderte Inhalte oder Werbung anzubieten. Beide Cookies können gleichartig sein (also Sitzungscookies oder persistente Cookies), ein vergleichbares Ablaufdatum aufweisen oder tatsächlich der Kontrolle Dritter unterliegen. Die Gefahr für den Datenschutz ergibt sich weniger aus den im Cookie enthaltenen Informationen als aus dem Zweck oder den Zwecken der Verarbeitung.

Letztlich muss also anhand des Zwecks und der konkreten Umsetzung oder Verarbeitung bestimmt werden, ob ein Cookie nach Kriterium A oder B von Einwilligungspflicht ausgenommen werden kann.

2.4 Mehrzweck-Cookies

Es ist zwar möglich, einen Cookie für verschiedene Zwecke zu verwenden, doch kann ein solcher Cookie nur dann von der Einwilligungspflicht ausgenommen werden, wenn jeder einzelne Zweck, zu dem der Cookie verwendet wird, von der Einwilligungspflicht ausgenommen ist.

So lässt sich beispielsweise ein Cookie mit einem eindeutigen Namen oder Wert erstellen, der sowohl zur Speicherung von Nutzereinstellungen als auch zum Zwecke des Tracking verwendet werden kann. Während für die Speicherung der Einstellungen des Nutzers unter bestimmten Umständen eine Ausnahme in Betracht kommt (vgl. Abschnitt 3.6), ist es höchst unwahrscheinlich, dass das Tracking eines der Kriterien A oder B erfüllt. Somit müsste die Website in jedem Fall die Einwilligung des Nutzers zum Tracking einholen. In der Praxis sollte dies die Betreiber von Websites dazu anregen, für jeden einzelnen Zweck einen anderen Cookie zu verwenden.

Wie die Datenschutzgruppe bereits in der Stellungnahme 16/2011 hervorgehoben hat, muss eine Website, die verschiedene Cookies oder verschiedenen Zwecken dienende Cookies verwendet, nicht für jeden einzelnen Cookie oder Zweck ein eigenes Banner oder eine eigene Einwilligungsanfrage anzeigen. Eine einzige klar und umfassend dargestellte Informations- und Einwilligungsseite reicht in den meisten Fällen aus.

³ Mithilfe einiger neuerer Technologien, die häufig als „Evercookies“ oder „Zombie-Cookies“ bezeichnet werden, ist es möglich, Cookies trotz geeigneter Lösversuche dauerhaft auf dem Endgerät des Nutzers zu speichern. Dass solche Cookies in irgendeinem Anwendungsfall von der Einwilligungspflicht ausgenommen wären, ist höchst unwahrscheinlich.

3 Anwendungsfälle für Cookies

In diesem Abschnitt werden die untersuchten Kriterien für die Ausnahme von der Einwilligungspflicht auf typische Anwendungsfälle für Cookies angewandt.

3.1 User-Input-Cookies

Der Begriff „User-Input-Cookies“ kann als Oberbegriff für Sitzungscookies gebraucht werden, die der einheitlichen Verfolgung von Nutzereingaben bei einer Reihe von Nachrichtenaustauschvorgängen mit einem Dienstleister dienen. In der Regel handelt es sich dabei um First-Party-Cookies, die sich gewöhnlich auf eine Session-ID (eine zufällige, temporäre, eindeutige Nummer) beziehen und spätestens zum Ende der Sitzung ablaufen.

Derartige Sitzungscookies werden normalerweise zum temporären Speichern von Nutzereingaben beim Ausfüllen von mehrseitigen Online-Formularen oder als Warenkorb zum temporären Speichern der vom Nutzer durch Anklicken einer Schaltfläche (z. B. „In den Warenkorb“) ausgewählten Artikel verwendet.

Diese Cookies sind eindeutig erforderlich, um einen vom Nutzer ausdrücklich gewünschten Dienst zur Verfügung zu stellen. Sie sind zudem mit einer Aktion des Nutzer (etwa dem Anklicken einer Schaltfläche oder dem Ausfüllen eines Formulars) verknüpft. Somit fallen diese Cookies unter die Ausnahmeregelung nach Kriterium B.

3.2 Authentifizierungsscookies

Authentifizierungsscookies werden verwendet, um den Nutzer zu identifizieren, nachdem er sich angemeldet hat (z. B. auf einer Online-Banking-Website). Diese Cookies werden benötigt, damit Nutzer sich bei aufeinanderfolgenden Besuchen einer Website authentifizieren und auf Inhalte, für die eine Zugriffsberechtigung erforderlich ist, wie etwa ihren Kontostand und Kontoumsätze zugreifen können. Authentifizierungsscookies sind in der Regel Sitzungscookies. Die Verwendung von persistenten Cookies ist ebenfalls möglich. Die beiden Arten dürfen jedoch, wie unten erörtert, nicht als identisch angesehen werden.

Wenn sich ein Nutzer anmeldet, fordert er ausdrücklich Zugriff auf Inhalte oder Funktionen, für die er eine Zugriffsberechtigung besitzt. Ohne ein im Cookie gespeichertes Authentifizierungstoken müsste der Nutzer bei jedem Seitenaufruf seinen Benutzernamen und sein Passwort eingeben. Die Authentifizierungsfunktion ist daher wesentlicher Bestandteil des von ihm ausdrücklich angeforderten Dienstes der Informationsgesellschaft. Somit fallen diese Cookies unter die Ausnahmeregelung nach Kriterium B.

Hier ist jedoch zu beachten, dass der Nutzer den Zugriff auf die Website und bestimmte Funktionen nur angefordert hat, um die von ihm benötigte Aufgabe ausführen zu können. Der Akt der Authentifizierung darf nicht dazu benutzt werden, den Cookie für andere sekundäre Zwecke wie Verhaltensüberwachung oder Werbung ohne Einwilligung zu verwenden.

Persistente Anmelde-Cookies, in denen ein Authentifizierungstoken über mehrere Browsersitzungen hinweg gespeichert wird, fallen nicht unter die Ausnahmeregelung nach Kriterium B. Dies ist ein wichtiger Unterschied, weil dem Nutzer unter Umständen nicht unmittelbar bewusst ist, dass die Authentifizierungseinstellungen durch das Schließen des Browsers nicht gelöscht werden. Er kehrt möglicherweise in der Annahme, jetzt anonym zu sein, auf die Website zurück, während er in Wirklichkeit nach wie vor bei dem Dienst

angemeldet ist. Eine Checkbox und ein einfacher Hinweis wie „Angemeldet bleiben (verwendet Cookies“), wie sie neben dem Anmeldeformular häufig zu sehen sind, stellen ein geeignetes Mittel zur Einholung der Einwilligung dar, so dass in diesem Fall eine Ausnahme nicht erforderlich ist.

3.3 Nutzerorientierte Sicherheitscookies

Die Ausnahmeregelung für Authentifizierungscookies nach Kriterium B (siehe oben) lässt sich auf andere Cookies ausdehnen, die ausschließlich der besseren Sicherheit des vom Nutzer ausdrücklich angeforderten Dienstes dienen. Dies betrifft beispielsweise Cookies, die verwendet werden, um wiederholt fehlgeschlagene Anmeldeversuche auf einer Website zu entdecken, oder andere ähnliche Mechanismen, die das Login-System vor Missbrauch schützen sollen (wenngleich dieser Schutz in der Praxis möglicherweise unzureichend ist). Diese Ausnahmeregelung würde sich jedoch nicht auf Cookies erstrecken, die der Sicherheit von Websites oder Diensten Dritter dienen, die nicht ausdrücklich vom Nutzer angefordert wurden.

Während Anmeldecookies in der Regel am Ende einer Sitzung ablaufen, sind nutzerorientierte Sicherheitscookies gewöhnlich länger gültig, um ihren Zweck erfüllen zu können.

3.4 Multimedia-Player-Sitzungscookies

Multimedia-Player-Sitzungscookies dienen der Speicherung von technischen Daten, die zur Wiedergabe von Video- oder Audio-Inhalten benötigt werden, wie etwa Bildqualität, Verbindungsgeschwindigkeit des Netzwerks und Pufferungsparameter. Diese Multimedia-Sitzungscookies werden nach der heutzutage am weitesten verbreiteten Internetvideotechnologie Adobe Flash allgemein als „Flash-Cookies“ bezeichnet. Da diese Informationen nicht über längere Dauer benötigt werden, laufen die Cookies normalerweise mit dem Ende der Sitzung ab.

Wenn der Nutzer eine Website mit verwandten Text- und Videoinhalten besucht, sind diese beiden Inhalte ebenfalls Teil eines vom Nutzer ausdrücklich angeforderten Dienstes. Die Videodisplayfunktion entspricht somit dem Kriterium B.

Wie bereits in Abschnitt 3.2 hervorgehoben wurde, müssen Betreiber von Websites, um die Ausnahmeregelung nutzen zu können, die Speicherung von für die Wiedergabe der Multimedia-Inhalte nicht unbedingt erforderlichen Zusatzinformationen in Flash-Cookies oder anderen Cookies vermeiden.

3.5 Lastverteilungs-Sitzungscookies

Die Lastverteilung ist ein Verfahren, das es ermöglicht, Webserveranfragen nicht von einem einzigen Server verarbeiten zu lassen, sondern auf einen Serverpool zu verteilen. Eine der Techniken zur Lastverteilung beruht auf einem sogenannten Load Balancer: Webanfragen von Nutzern werden an einen Lastverteilungsserver geschickt, der sie an einen verfügbaren internen Server im Pool weiterleitet. In manchen Fällen darf diese Weiterleitung während einer Sitzung nicht verändert werden: Sämtliche Anfragen von einem bestimmten Nutzer müssen zur Gewährleistung einer einheitlichen Verarbeitung stets an denselben Server im Pool weitergeleitet werden. Neben verschiedenen anderen Techniken kann ein Cookie verwendet werden, um den Server im Pool zu identifizieren und zu gewährleisten, dass der Load Balancer die Anfragen korrekt weiterleitet. Diese Cookies sind Sitzungscookies.

Die im Cookie enthaltenen Informationen dienen dem alleinigen Zweck, die Verbindungsendpunkte (einen der Server im Pool) zu identifizieren und sind daher für die Übertragung der Nachricht über das Netz erforderlich. Somit fallen diese Cookies unter die Ausnahmeregelung nach Kriterium A.

3.6 Cookies zur Anpassung der Benutzeroberfläche

Cookies zur Anpassung der Benutzeroberfläche werden verwendet, um die nicht mit einer anderen dauerhaften Kennung wie etwa einem Benutzernamen verknüpften Einstellungen eines Nutzers für einen mehrere Webseiten umfassenden Dienst zu speichern. Sie werden nur dann verwendet, wenn der Nutzer den Dienst beispielsweise durch Anklicken einer Schaltfläche oder Markieren eines Feldes ausdrücklich aufgefordert hat, eine bestimmte Information zu speichern. Sie können je nach Zweck Sitzungscookies sein oder mehrere Wochen oder Monate gültig sein.

Typische Beispiele für Anpassungscookies:

- Cookies für Spracheinstellungen, die verwendet werden, um die von einem Nutzer auf einer mehrsprachigen Website (etwa durch Anklicken einer „Flagge“) ausgewählte Sprache zu speichern.
- Cookies für die Darstellung von Suchergebnissen, die verwendet werden, um die Einstellungen des Nutzers für Online-Suchanfragen (z. B. die Anzahl der Ergebnisse pro Seite) zu speichern.

Diese Anpassungsfunktionen werden somit vom Nutzer eines Dienstes der Informationsgesellschaft ausdrücklich aktiviert (etwa durch Anklicken einer Schaltfläche oder Markieren eines Feldes), wenngleich bei Fehlen zusätzlicher Hinweise die Absicht des Nutzers nicht dahingehend interpretiert werden kann, dass die Auswahl über eine Browsersitzung hinaus (oder länger als einige Stunden) gespeichert werden soll. Somit fallen nur Sitzungs- oder Kurzzeitcookies zur Speicherung solcher Informationen unter die Ausnahmeregelung nach Kriterium B. Durch einen auffälligen Hinweis (etwa „verwendet Cookies“ neben der Flagge) wäre der Aufklärungspflicht für eine gültige Einwilligung in die längerfristige Speicherung der Einstellungen des Nutzers Genüge getan und eine Ausnahmeregelung für diesen Fall nicht erforderlich.

3.7 Content-Sharing-Cookies sozialer Plugins

Viele soziale Netzwerke bieten soziale Plugin-Module, die Betreiber von Websites in ihre Plattform integrieren können, um vor allem den Nutzern sozialer Netzwerke die Möglichkeit zu geben, Inhalte, die ihnen gefallen, mit ihren „Freunden“ zu teilen (und ihnen damit zusammenhängende Funktionen wie die Veröffentlichung von Kommentaren anzubieten). Diese Plugins speichern im Endgerät des Nutzers Cookies und greifen darauf zu, damit das soziale Netzwerk in der Interaktion mit diesen Plugins seine Mitglieder identifizieren kann.

Bei diesem Anwendungsfall ist unbedingt zwischen Nutzern, die über ihren Browser bei einem bestimmten sozialen Netzwerk „angemeldet“ sind, und „nicht angemeldeten“ Nutzern, die entweder kein Mitglied des betreffenden Netzwerks sind oder sich von ihrem sozialen Netzwerk „abgemeldet“ haben, zu unterscheiden.

Da soziale Plugins definitionsgemäß für die Mitglieder eines bestimmten sozialen Netzwerks bestimmt sind, haben sie für Nichtmitglieder keinerlei Nutzen und entsprechen somit für diese Nutzer nicht dem Kriterium B. Dies gilt auch für Mitglieder eines sozialen Netzwerks, die sich von der Plattform ausdrücklich „abgemeldet“ haben und daher nicht damit rechnen, wieder mit dem sozialen Netzwerk „verbunden“ zu werden. Deshalb ist die Einwilligung von Nichtmitgliedern und „abgemeldeten“ Mitgliedern erforderlich, bevor soziale Plugins Third-Party-Cookies verwenden dürfen.

Andererseits erwarten viele „angemeldete“ Nutzer, dass sie auf Websites Dritter soziale Plugins nutzen und darauf zugreifen können. In diesem speziellen Fall ist der Cookie für eine vom Nutzer ausdrücklich gewünschte Funktionalität unbedingt erforderlich, und Kriterium B trifft zu. Derartige Cookies sind Sitzungscookies⁴: Damit sie ihren besonderen Zweck erfüllen, müssen sie ablaufen, wenn sich der Nutzer von seinem sozialen Netzwerk abmeldet oder der Browser geschlossen wird. Soziale Netzwerke, die Cookies über Kriterium B hinaus für weitere Zwecke (oder über eine längere Gültigkeitsdauer) verwenden möchten, haben reichlich Gelegenheit, ihre Mitglieder auf der Plattform des sozialen Netzwerks selbst darüber zu informieren und ihre Einwilligung einzuholen.

4 Von der Einwilligungspflicht nicht ausgenommene Cookies

Dieser Abschnitt zeigt nicht unter die Ausnahmeregelung nach Kriterium A oder B fallende Cookie-Anwendungen erneut auf oder präzisiert sie.

4.1 Tracking-Cookies sozialer Plugins

Wie bereits beschrieben, bieten viele soziale Netzwerke soziale Plugin-Module, die Besitzer von Websites in ihre Plattform integrieren können, um bestimmte Dienste zu erbringen, von denen angenommen wird, dass sie von den Mitgliedern der sozialen Netzwerke „ausdrücklich gewünscht“ werden. Allerdings können diese Module auch verwendet werden, um die Aktivitäten von Mitgliedern wie auch Nichtmitgliedern mithilfe von Third-Party-Cookies für weitere Zwecke wie etwa verhaltensorientierte Werbung, Analysen oder Marktforschung zu verfolgen.

In diesen Fällen können solche Cookies nicht als für eine vom Nutzer ausdrücklich gewünschte Funktion „*unbedingt erforderlich*“ angesehen werden. Daher können diese Tracking-Cookies nicht unter die Ausnahmeregelung nach Kriterium B fallen. Es ist unwahrscheinlich, dass es ohne die Einholung der Einwilligung irgendeine Rechtsgrundlage gibt, die es sozialen Netzwerken erlaubt, mithilfe sozialer Plugins Daten über Nichtmitglieder des jeweiligen Netzwerks zu sammeln. Soziale Plugins sollten deshalb auf Seiten, die Nichtmitgliedern angezeigt werden, standardmäßig keine Third-Party-Cookies setzen. Andererseits haben soziale Netzwerke, wie bereits ausgeführt, reichlich Gelegenheit, die Einwilligung ihrer Mitglieder zu einem derartigen Tracking direkt auf ihrer Plattform einzuholen, nachdem sie sie klar und umfassend darüber informiert haben.

4.2 Third-Party-Cookies zu Werbezwecken

Wie die Datenschutzgruppe in ihren Stellungnahmen 2/2010 und 16/2011 bereits ausführlich dargelegt hat, sind Third-Party-Cookies, die der verhaltensorientierten Werbung dienen, nicht von der Einwilligungspflicht ausgenommen. Diese Pflicht zur Einholung der Einwilligung

⁴ Wie in Abschnitt 3.2 gezeigt wurde, fallen persistente Authentifizierungsscookies nicht unter die Ausnahmeregelung.

erstreckt sich naturgemäß auf alle in der Werbung zu betrieblichen Zwecken verwendeten Third-Party-Cookies. Hierzu zählen unter anderem Cookies zum Zweck des Frequency Capping, der Protokollierung von Finanzdaten, des Affiliate-Marketing, der Erkennung von Klickbetrug, der Marktforschung und Marktanalyse, der Produktverbesserung und der Fehlerbehebung, denn keiner dieser Zwecke steht im Zusammenhang mit einem vom „Nutzer ausdrücklich gewünscht[en]“ Dienst der Informationsgesellschaft oder einer Funktion eines solchen Dienstes, wie in Kriterium B vorgesehen.

In diesem Zusammenhang beteiligt sich die Datenschutzgruppe seit dem 22. Dezember 2011 aktiv an der Arbeit des World Wide Web Consortiums (W3C) zur Standardisierung der Technologie und der Bedeutung von „Do Not Track“. In Anbetracht dessen, dass Cookies oft eindeutige Kennungen enthalten, die eine Verfolgung des Nutzerverhaltens über einen gewissen Zeitraum und mehrere Websites hinweg ermöglichen, sowie der möglichen Kombination dieser Kennungen mit anderen der Identifizierung dienenden oder identifizierbaren Daten ist die Datenschutzgruppe besorgt über einen eventuellen Ausschluss von „Do Not Track“ von bestimmten für betriebliche Zwecke als notwendig erachteten Cookies. Solche Zwecke sind Frequency Capping, Financial Logging (Protokollierung von Finanzdaten), 3rd Party Auditing (Prüfungen durch Dritte), Security (Sicherheitszwecke), Contextual Content (Bereitstellung kontextbezogener Inhalte), Research and Market Analytics (Marktforschung und -analysen), Product Improvement and Debugging (Produktverbesserung und Fehlerbehebung)⁵. Damit der Standard „Do Not Track“ dazu führt, dass Unternehmen, die bei europäischen Bürgern Cookies setzen, vorschriftskonform handeln, muss „Do Not Track“ faktisch und ausnahmslos „Nicht erfassen“ bedeuten. Wenn also ein Nutzer zum Ausdruck gebracht hat, dass er kein Tracking wünscht (DNT=1), darf keine Kennung zu Tracking-Zwecken gesetzt oder anderweitig verarbeitet werden. Technische Lösungen, die im Webbrowser und auf der Serverseite einen effektiven Datenschutz durch Technik bewirken und die oben genannten betrieblichen Zwecke erreichen, stehen bereits zur Verfügung, und viele weitere werden derzeit entwickelt.

4.3 First-Party-Analysecookies

Webanalysen sind statistische Zielgruppen-Tools für Websites, die häufig auf Cookies angewiesen sind. Diese Tools werden vor allem von Websitebesitzern verwendet, um die Zahl der Einzelbesucher zu schätzen, die wichtigsten Suchbegriffe, die über Suchmaschinen zu einer Website führen, zu ermitteln oder Navigationsprobleme der Website aufzuspüren. Die Analysetools von heute verwenden zahlreiche unterschiedliche Modelle zur Datenerfassung und -analyse, die jeweils unterschiedliche Datenschutzrisiken aufweisen. Ein auf First-Party-Cookies gestütztes Analysesystem des Erstanbieters beinhaltet fraglos andere Risiken als ein auf Third-Party-Cookies gestütztes externes Analysesystem. Ferner gibt es Tools, die First-Party-Cookies verwenden, während die Analysen von einem Dritten durchgeführt werden. Dieser Dritte gilt je nachdem, ob er die Daten für eigene Zwecke oder – wenn dies unzulässig ist – aufgrund technischer oder vertraglicher Regelungen nutzt, als gemeinsam für die Verarbeitung Verantwortlicher oder als Auftragsverarbeiter.

Während diese Tools häufig als „unbedingt erforderlich“ für Betreiber von Websites angesehen werden, sind sie für eine vom Nutzer (oder Teilnehmer) ausdrücklich gewünschte Funktion nicht unbedingt erforderlich. Genau genommen kann der Nutzer auch dann auf alle Funktionen der Website zugreifen, wenn derartige Cookies deaktiviert sind. Folglich fallen diese Cookies nicht unter die Ausnahmeregelung nach Kriterium A oder B.

⁵ <http://www.w3.org/TR/tracking-compliance/>

Allerdings stellen First-Party-Analysecookies nach Ansicht der Datenschutzgruppe kaum ein Datenschutzrisiko dar, wenn sie ausschließlich für die aggregierten Statistiken des Erstanbieters genutzt und von Websites verwendet werden, die in ihrer Datenschutzrichtlinie bereits unmissverständlich über diese Cookies informieren und ausreichende Datenschutzgarantien bieten. Diese Garantien sollten unter anderem eine benutzerfreundliche Möglichkeit zur Abwahl jedweder Datenerfassung sowie umfassende Anonymisierungsmechanismen für sonstige gesammelte Informationen wie etwa IP-Adressen, anhand derer Personen identifiziert werden können, beinhalten.

In diesem Zusammenhang könnte der europäische Gesetzgeber im Falle einer künftigen Überarbeitung von Artikel 5 Absatz 3 der Richtlinie 2002/58/EG in geeigneter Weise ein drittes Kriterium für die Ausnahme von der Einwilligungspflicht für Cookies aufnehmen, die ausschließlich der Erstellung anonymisierter und aggregierter Statistiken des Erstanbieters dienen.

Analysen des Erstanbieters sind klar von externen Analysen zu unterscheiden, weil letztere gängige Third-Party-Cookies verwenden, um Navigationsdaten von Nutzern über verschiedene Websites hinweg zu sammeln, und somit ein wesentlich größeres Datenschutzrisiko darstellen.

5 Zusammenfassung und Leitlinien

Diese Analyse hat gezeigt, dass folgende Cookies unter bestimmten Bedingungen von der Einwilligung in Kenntnis der Sachlage ausgenommen werden können, sofern sie nicht für weitere Zwecke verwendet werden:

- 1) User-Input-Cookies (Session-ID) für die Dauer einer Sitzung oder in bestimmten Fällen persistente Cookies, deren Gültigkeitsdauer auf wenige Stunden beschränkt ist,
- 2) Authentifizierungscookies für Dienste, bei denen eine Authentifizierung erforderlich ist, für die Dauer einer Sitzung,
- 3) nutzerorientierte Sicherheitscookies zur Erkennung von Authentifizierungsmissbrauch für eine begrenzte längere Dauer,
- 4) Multimedia-Player-Sitzungscookies wie Flash-Player-Cookies für die Dauer einer Sitzung,
- 5) Lastverteilungs-Sitzungscookies für die Dauer der Sitzung,
- 6) persistente Cookies zur Anpassung der Benutzeroberfläche für die Dauer einer Sitzung (oder etwas länger),
- 7) Third-Party-Content-Sharing-Cookies sozialer Plugins für angemeldete Mitglieder eines sozialen Netzwerks.

Im Zusammenhang mit sozialen Netzwerken weist die Datenschutzgruppe jedoch darauf hin, dass die Verwendung von Third-Party-Cookies in sozialen Plugins, die anderen Zwecken als der Bereitstellung einer von den Mitgliedern des betreffenden Netzwerks ausdrücklich gewünschten Funktion dienen, der Einwilligung bedarf, insbesondere wenn es darum geht, das Verhalten von Nutzern über mehrere Websites hinweg zu verfolgen.

Die Datenschutzgruppe erinnert daran, dass Third-Party-Cookies, die Werbezwecken dienen, nicht von der Einwilligungspflicht ausgenommen werden können, und stellt weiter klar, dass eine Einwilligung auch erforderlich ist, wenn die Cookies für betriebliche Zwecke im Zusammenhang mit Werbung Dritter (wie Frequency Capping, Protokollierung von Finanzdaten, Affiliate-Marketing, Erkennen von Klickbetrug, Marktforschung und -analysen, Produktverbesserung und Fehlerbehebung) verwendet werden. Wenngleich bei manchen betrieblichen Zwecken sicherlich zwischen einzelnen Nutzern unterschieden werden muss, rechtfertigen diese Zwecke grundsätzlich nicht die Verwendung eindeutiger Kennungen. Dieser Aspekt ist vor allem vor dem Hintergrund der aktuellen Diskussion über die Umsetzung des Standards „Do Not Track“ in Europa von besonderer Bedeutung.

Diese Analyse zeigt auch, dass First-Party-Analysecookies nicht von der Einwilligungspflicht ausgenommen sind, aber nur ein begrenztes Datenschutzrisiko darstellen, sofern angemessene Datenschutzgarantien wie ausreichende Information der Nutzer, einfache Abwahlmöglichkeiten und umfassende Anonymisierungsmechanismen vorhanden sind.

Aus der Analyse und den in dieser Stellungnahme vorgestellten Anwendungsfällen für Cookies lassen sich einige grundlegende Regeln ableiten:

- 1) Bei der Anwendung von Kriterium B ist zu prüfen, was aus Sicht des Nutzers, nicht des Diensteanbieters, unbedingt erforderlich ist.
- 2) Wird ein Cookie für verschiedene Zwecke verwendet, kann er nur dann von der Einwilligung in Kenntnis der Sachlage ausgenommen werden, wenn jeder einzelne Zweck davon ausgenommen ist.
- 3) First-Party-Sitzungscookies sind mit wesentlich höherer Wahrscheinlichkeit von der Einwilligungspflicht ausgenommen als persistente Third-Party-Cookies. Bei der Beurteilung, ob für einen Cookie die Ausnahmeregelung gilt, sollte jedoch stets der Zweck des Cookies und nicht eines seiner technischen Merkmale zugrunde gelegt werden.

Um abschließend entscheiden zu können, ob ein Cookie von der grundsätzlichen Pflicht zur Einholung einer Einwilligung in Kenntnis der Sachlage ausgenommen ist, muss sorgfältig geprüft werden, ob es einem der beiden Ausnahmekriterien entspricht, die der durch die Richtlinie 2009/136/EG geänderte Artikel 5 Absatz 3 festlegt. Bestehen auch nach sorgfältiger Prüfung noch erhebliche Zweifel daran, ob eines der Ausnahmekriterien anwendbar ist, sollte der Websitebetreiber eingehend prüfen, ob es nicht praktisch möglich ist, die Einwilligung der Nutzer auf einfache und unaufdringliche Weise einzuholen und somit jegliche Rechtsunsicherheit zu vermeiden.

Brüssel, den 7. Juni 2012

Für die Datenschutzgruppe
Der Vorsitzende
Jacob KOHNSTAMM