00879/12/EN
WP 194

Cookie Einwilligungs-Befreiung

Opinion 04/2012 on Cookie Consent Exemption

Adopted on 7 June 2012

Hier wird die EU-Cookie-Richtlinie (Stand 2009 !!!) beleuchtet:
Wann genau ist ein Cookie von der Einwilligungspflicht befreit?

Die engen Kriterien der Richtlinie werden hier streng ausgelegt.
In den allermeisten Fällen muss eine Einwilligung eingeholt werden.
Auf Seite 11 ist das Ergebnis zu lesen.

ABER:

Auf Seite 10 findet sich die Forderung nach einer weiteren Befreiung:
Für Cookies zur internen Nutzungsprofil-Erstellung !!!
Das ist der Grund, warum der § 15 Abs. 3 TMG unionsrechtskonform war.

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1(a) and 3 of that Directive,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT OPINION

1 Introduction

Article 5.3 of Directive 2002/58/EC, as amended by Directive 2009/136/EC has reinforced the protection of users of electronic communication networks and services by requiring informed consent before information is stored or accessed in the user's (or subscriber's) terminal device. The requirement applies to all types of information stored or accessed in the user's terminal device although the majority of discussion has centred on the usage of cookies as understood by the definition in RFC6265[1]. As such, this opinion explains how the revised Article 5.3 impacts on the usage of cookies but the term should not be regarded as excluding similar technologies.

Article 5.3 allows cookies to be exempted from the requirement of informed consent, if they satisfy one of the following criteria:

CRITERION A: the cookie is used "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network*".

CRITERION B: the cookie is "*strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*".

While the requirements for informed consent were already examined in detail by the Working Party in two Opinions[2], this document is designed to analyze the exemptions to this principle, in the context of cookies and related technologies.

This analysis is conducted without prejudice to the right to be informed and the eventual right to oppose set forth by Directive 95/46/EC, which apply to personal data processing whether cookies are used or not.

2 Analysis

2.1 Criterion A

The inclusion of the phrase "sole purpose" in CRITERION A specifically limits the types of processing which may be undertaken using cookies and does not leave much room for

[1] http://tools.ietf.org/html/rfc6265

[2] Opinion 2/2010 on "*online behavioural advertising*" 2/2010 and in Opinion 16/2011 on "*the EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*". WP-171 und WP-188

interpretation. Simply using a cookie to assist, speed up or regulate the transmission of a communication over an electronic communications network is not sufficient. The transmission of the communication must not be possible without the use of the cookie. It can be noted that in the original version of Directive 2002/58/EC, Article 5.3 already included this exemption for cookies that were used "*for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network*". The same wording was used in the revised directive, but the words "*or facilitating*" were removed, which could be interpreted as a further indication that the European Legislator intended to restrict the perimeter of the exemption afforded by Article 5.3 under CRITERION A.

At least 3 elements that can be considered as strictly necessary for communications to take place over a network between two parties:

1) The ability to route the information over the network, notably by identifying the communication endpoints.

2) The ability to exchange data items in their intended order, notably by numbering data packets,

3) The ability to detect transmission errors or data loss.

The terms "*the transmission of a communication over an electronic communications network"* in CRITERION A –and in particular the word "*over*"– are understood to refer to any type of data exchange that takes place with the use of an electronic communication network (as defined in Directive 2002/21/EC), potentially including "application level" data which fulfills at least one of the properties defined above, without limitation to technical data exchanges needed to establish the electronic communication network itself.

As such, CRITERION A encompasses cookies that fulfil at least one of the properties defined above for Internet communications.

2.2 Criterion B

Similarly, the wording of CRITERION B suggests that the European Legislator intended to ensure that the test for qualifying for such an exemption must remain high. Following a direct reading of the directive, a cookie matching CRITERION B has to pass simultaneously the two following tests:

1) The information society service has been explicitly requested by the user: the user (or subscriber) did a positive action to request a service with a clearly defined perimeter.

2) The cookie is strictly needed to enable the information society service: if cookies are disabled, the service will not work.

Furthermore, recital 66 of Directive 2009/136/EC underlines that "*Exceptions to the obligation to provide information and offer the right to refuse should be limited to those situations where the technical storage or access is strictly necessary for the legitimate purpose of enabling the use of a specific service explicitly requested by the subscriber or user.*" In other words, there has to be a clear link between the strict necessity of a cookie and the delivery of the service explicitly requested by the user for the exemption to apply.

Even with such a reading of the directive, it remains to define what constitutes the scope of an "*information society service explicitly requested by the subscriber or user"*. An information society service can be composed of many components, some of which are not used by all users or are provided for convenience. For example, an online newspaper can be free to access for all, but may provide some additional functionalities for users that are "logged-in" such as the ability to leave comments on articles. In turn these additional functionalities may operate with their own cookies. In this particular context, the Working Party considers that an information society service should be viewed as the sum of several functionalities, and that the precise scope of such a service may thus vary according to the functionalities requested by the user (or subscriber).

As a consequence, CRITERION B can be rewritten in terms of "functionalities" provided by an information society service. In these terms, a cookie matching CRITERION B would need to pass the following tests:

1) A cookie is necessary to provide a specific functionality to the user (or subscriber): if cookies are disabled, the functionality will not be available.

2) This functionality has been explicitly requested by the user (or subscriber), as part of an information society service.

2.3 Characteristics of a cookie

Cookies are often categorized according to the following characteristics:

1) Whether they are "session cookies" or "persistent cookie".

2) Whether they are "third party cookies" or not.

A "session cookie" is a cookie that is automatically deleted when the user closes his browser, while a "persistent cookie" is a cookie that remains stored in the user's terminal device until it reaches a defined expiration date (which can be minutes, days or several years in the future).

The term "third party cookie" can be misleading:

- In the context of European data protection, the Directive 95/46/EC defines a third party as "*any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.*" A "third party cookie" would thus refer to a cookie set by a data controller that is distinct from the one that operates the website visited by the user (as defined by the current URL displayed in the address bar of the browser).

- However, from the perspective of browsers, the notion of "third party" is solely defined by looking at the structure of the URL displayed in the address bar of the browser. In this case "third party cookies" are cookies that are set by websites that belong to a domain that is distinct from the domain of the website visited by the user as displayed in the browser address bar, regardless of any consideration whether that entity is a distinct data controller or not.

While these two approaches often overlap, they are not always equivalent. For the purpose of this opinion, we will follow the first approach and use the term "third party cookie" to describe cookies that are set by data controllers that do not operate the website currently visited by the user. Conversely, the term "first party cookie" will be used to refer to a cookie set by the data controller (or any of its processors) operating the website visited by the user, as defined by the URL that is usually displayed in the browser address bar.

Certain characteristics will be taken into account to evaluate if a cookie is "*strictly necessary*" for a service, "*explicitly requested by the user*" or limited to a "*sole purpose*" as worded in CRITERION A or B.

A cookie that is exempted from consent should have a lifespan that is in direct relation to the purpose it is used for, and must be set to expire once it is not needed, taking into account the reasonable expectations of the average user or subscriber. This suggests that cookies that match CRITERION A and B will likely be cookies that are set to expire when the browser session ends or even earlier. However, this is not always the case. For example, in the shopping basket scenario presented in the following section, a merchant could set the cookie either to persist past the end of the browser session or for a couple of hours in the future to take into account the fact that the user may accidentally close his browser and could have a reasonable expectation to recover the contents of his shopping basket when he returns to the merchant's website in the following minutes. In other cases, the user may explicitly ask the service to remember some information from one session to another, which requires the use of persistent cookies to fulfil that purpose.

Additionally, following the previous definitions, "third party" cookies are usually not "*strictly necessary*" to the user visiting a website since these cookies are usually related to a service that is distinct from the one that has been "*explicitly requested*" by the user.

As a consequence, "first party" session cookies are far more likely to be exempted from consent than "third party" persistent[3] cookies. But while these characteristics may serve as an initial indicator to prioritize compliance actions, they are not sufficient alone to establish if a cookie matches CRITERION A or B. One can imagine a cookie being used to authenticate users logging into a website. This cookie is used to ensure that the user may only access content to which they are authorized. A similar cookie may be used to identify and track users across a domain and deliver tailored content or advertising based on the profile held by the website operator. Both cookies may be similar in type (i.e. session or persistent); have a similar expiration date; or indeed be controlled by third parties. The risk to data protection comes from the purpose(s) of processing rather than the information contained within the cookie.

Ultimately, it is thus the purpose and the specific implementation or processing being achieved that must be used to determine whether or not a cookie can be exempted from consent according to CRITERION A or B.

[3] Some recent technologies often referred as "Ever-cookies" or "Zombie-cookies" allow cookies to remain permanently on the user's terminal device despite reasonable efforts to remove them. It is very unlikely that such cookies would be exempted from consent under any scenario.

2.4 Multipurpose cookies

While it is possible to use a cookie for several purposes, such a cookie may only be exempted from consent if all the distinct purposes for which the cookie is used are individually exempted from consent.

For example, it is possible to create a cookie that has a unique name or value that can both be used for the purpose of remembering user preferences and for the purpose of tracking. While remembering the user's preferences may be considered in some circumstances to fall under an exemption (as illustrated in section 3.6), tracking is very unlikely to meet CRITERION A or B. As such, the website would still need to seek user consent for the tracking purpose. In practice, this should encourage website owners to use a different cookie for each distinct purpose.

As already highlighted by the Working Party in Opinion 16/2012, if a website uses several cookies or cookies that cover several purposes, this does not mean that it must present a separate "banner" or consent request for each cookie or purpose. A single point of information and consent, presented in a clear and comprehensive manner is sufficient in most cases.

3 Cookie use case scenarios

This section applies the previously analyzed consent exemption criteria to common cookie use case scenarios.

3.1 "User-input" cookies

The term "user input cookies" can be used as a generic term to describe session cookies that are used to keep track of the user's input in a series of message exchanges with a service provider in a consistent manner. These would be expected to be first party cookies typically relying on a Session-ID (a random temporary unique number) and expire when the session ends at the latest.

First party user input session cookies are typically used to keep track of the user's input when filling online forms over several pages, or as a shopping cart, to keep track of the items the user has selected by clicking on a button (e.g. "add to my shopping cart").

These cookies are clearly needed to provide an information service explicitly requested by the user. Additionally, they are tied to a user's action (such as clicking on a button or filling a form). As such these cookies are exempted under CRITERION B.

3.2 Authentication cookies

Authentication cookies are used to identify the user once he has logged in (example: on an online banking website). These cookies are needed to allow users to authenticate themselves on successive visits to the website and gain access to authorized content, such as viewing their account balance, transactions, etc. Authentication cookies are usually session cookies. The use of persistent cookies is also possible but they must not be regarded as identical, as discussed below.

When a user logs in, he explicitly requests access to the content or functionality to which he is authorized. Without the use of an authentication token stored in a cookie the user would have to provide a username/password on each page request. Therefore this authentication functionality is an essential part of the information society service he is explicitly requesting. As such these cookies are exempted under CRITERION B.

However it is important to note that the user has only requested access to the site and specific functionality to perform the task he requires. The act of authentication must not be taken as an opportunity to use the cookie for other secondary purposes such as behavioural monitoring or advertising without consent.

Persistent login cookies which store an authentication token across browser sessions are not exempted under CRITERION B. This is an important distinction because the user may not be immediately aware of the fact that closing the browser will not clear their authentication settings. They may return to the website under the assumption that they are anonymous whilst in fact they are still logged in to the service. The commonly seen method of using a checkbox and a simple information note such as "remember me (uses cookies)" next to the submit form would be an appropriate means of gaining consent therefore negating the need to apply an exemption in this case.

3.3 User centric security cookies

The exemption that applies to authentication cookies under CRITERION B (as previously described) can be extended to other cookies set for the specific task of increasing the security of the service that has been explicitly requested by the user. This is the case for example for cookies used to detect repeated failed login attempts on a website, or other similar mechanisms designed to protect the login system from abuses (though this may be a weak safeguard in practice). This exemption would not however cover the use of cookies that relate to the security of websites or third party services that have not been explicitly requested by the user.

While login cookies are typically set to expire at the end of a session, user security cookies are expected to have a longer lifespan to fulfil their security purpose.

3.4 Multimedia player session cookies

Multimedia player session cookies are used to store technical data needed to play back video or audio content, such as image quality, network link speed and buffering parameters. These multimedia session cookies are commonly known as "flash cookies", so called because the most prevalent internet video technology in use today is Adobe Flash. As there is no long-term need for this information they should expire once the session ends.

When the user visits a website containing related text and video contents, both of these contents are equally part of a service explicitly requested by the user. The video display functionality thus matches CRITERION B.

As already highlighted in Section 3.2, to benefit from the exemption, website operators must avoid the inclusion of additional information into the "flash" or other cookies which are not strictly necessary for the playback of the media content.

3.5 Load balancing session cookies

Load balancing is a technique that allows distributing the processing of web server requests over a pool of machines instead of just one. One of the techniques that are used to achieve load balancing is based on a "load balancer": web requests from the users are directed to a load balancing gateway which forwards the request to one of the available internal servers in the pool. In some cases, this redirection needs to be persistent during a session: all requests originating from a specific user must always be forwarded to the same server in the pool to maintain the consistency of the processing. Among several techniques, a cookie may be used to identify the server in the pool in order for the load balancer to redirect the requests appropriately. These are session cookies.

The information in the cookie has the sole purpose of identifying one of the communication endpoints (one of the servers in the pool) and is thus necessary to carry out the communication over the network. As such these cookies are exempted under CRITERION A.

3.6 UI customization cookies

User interface customization cookies are used to store a user's preference regarding a service across web pages and not linked to other persistent identifiers such as a username. They are only set if the user has explicitly requested the service to remember a certain piece of information, for example, by clicking on a button or ticking a box. They may be session cookies or have a lifespan counted in weeks or months, depending on their purpose.

Typical examples of customization cookies are:

- Language preference cookies that are used to remember the language selected by a user on a multilingual website (e.g. by clicking on a "flag").

- Result display preference cookies that are used to remember the user's preference regarding online search queries (e.g. by selecting the number of results per page).

These customization functionalities are thus explicitly enabled by the user of an information society service (e.g. by clicking on button or ticking a box) although in the absence of additional information the intention of the user could not be interpreted as a preference to remember that choice for longer than a browser session (or no more than a few additional hours). As such only session (or short term) cookies storing such information are exempted under CRITERION B. The addition of additional information in a prominent location (e.g. "uses cookies" written next to the flag) would constitute sufficient information for valid consent to remember the user's preference for a longer duration, negating the requirement to apply an exemption in this case.

3.7 Social plug-in content sharing cookies

Many social networks propose "social plug-in modules" that website operators can integrate in their platform notably to allow social networks users to share contents they like with their "friends" (and propose other related functionalities such as publishing comments). These plug-ins store and access cookies in the user's terminal equipment in order to allow the social network to identify their members when they interact with these plug-ins.

To address this use case, it is important to distinguish users who "logged-in" through their browser in a particular social network account, from "non-logged-in" users who are either simply not a member of that specific social network or who have "disconnected" from their social network account.

Since by definition social plug-ins are destined to members of a particular social network, they are not of any use for non members, and therefore do not match CRITERION B for those users. This can be extended to actual members of a social network who have explicitly "logged-out" of the platform, and as such do not expect to be "connected" to the social network anymore. Consent from non-members and "logged-out" members is thus needed before third party cookies can be used by social plug-ins.

On the other hand, many "logged in" users expect to be able to use and access social plug-ins on third party websites. In this particular case, the cookie is strictly necessary for a functionality explicitly requested by the user and CRITERION B applies. Such cookies are session cookies[4]: to serve their particular purpose, their lifespan should end when the user "logs-out" of his social network platform or if the browser is closed. Social networks that wish to use cookies for additional purposes (or a longer lifespan) beyond CRITERION B have ample opportunity to inform and gain consent from their members on the social network platform itself.

4 Non exempted cookies

This section recalls or clarifies cookie usage scenarios do not fall in the exemption afforded under CRITERION A or B.

4.1 Social plug-in tracking cookies

As described previously, many social networks propose "social plug-in modules" that website owners can integrate in their platform, to provide some services than can be considered as "explicitly requested" by their members. However these modules can also be used to track individuals, both members and non-members, with third party cookies for additional purposes such as behavioural advertising, analytics or market research, for example.

With such purposes, these cookies cannot be deemed to be "*strictly necessary"* to provide a functionality explicitly requested by the user. Therefore these tracking cookies cannot be exempted under CRITERION B. Without consent, it seems unlikely that there is any legal basis for social networks to collect data through social plug-ins about non-members of their network. By default, social plug-ins should thus not set a third party cookie in pages displayed to non-members. On the other hand, as previously noted, social networks have ample opportunity to collect consent from their members directly on their platform if they wish to conduct such tracking activities, having provided their users with clear and comprehensive information about this activity.

4.2 Third party advertising

Third party cookies used for behavioural advertising are not exempted from consent as already highlighted in detail by the Working Party in Opinion 2/2010 and Opinion 16/2011. This requirement for consent naturally extends to all related third party operational cookies

[4] Persistent authentication cookies have been demonstrated to be not exempt in section 3.2

used in advertising including cookies used for the purpose of frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging, as neither of these purposes can be considered to be related to a service or functionality of an information society service *explicitly requested by the user*, as required by CRITERION B.

In this regard, the Working Party has been actively participating since December 22, 2011 in the work of the World Wide Web Consortium (W3C) to standardize the technology and the meaning of Do Not Track. In view of the fact that cookies often contain unique identifiers, that allow for the tracking of user behaviour over time and across websites and the possible combination of these identifiers with other identifying or identifiable data, the Working Party is concerned about the possible exclusion from Do Not Track of certain cookies that are said to be necessary for operational purposes. Such purposes are: Frequency Capping, Financial Logging, 3rd Party Auditing, Security, Contextual Content, Research and Market Analytics, Product Improvement and Debugging[5]. In order for the Do Not Track standard to bring compliance to companies serving cookies to European citizens, Do Not Track must effectively mean "*Do Not Collect*" without exceptions. Therefore where a user has expressed the preference to not be tracked (DNT=1) no identifier, for the purpose of tracking, must be set or otherwise processed. There are technical solutions available, and many more are currently being developed, to effectively apply privacy by design, both within the web browser and on the server side to achieve the operational purposes described above.

4.3 First party analytics Das hier ist wichtig für Google-Analytics, econda etc.

Analytics are statistical audience measuring tools for websites, which often rely on cookies. These tools are notably used by website owners to estimate the number of unique visitors, to detect the most preeminent search engine keywords that lead to a webpage or to track down website navigation issues. Analytics tools available today use a number of different data collection and analysis models each of which present different data protection risks. A first-party analytic system based on "first party" cookies clearly presents different risks compared to a third-party analytics system based on "third party" cookies. There are also tools which use "first party" cookies with the analysis performed by another party. This other party will be considered as a joint controller or as a processor depending on whether it uses the data for its own purposes or if it is prohibited to do so through technical or contractual arrangements.

While they are often considered as a "strictly necessary" tool for website operators, they are not strictly necessary to provide a functionality explicitly requested by the user (or subscriber). In fact, the user can access all the functionalities provided by the website when such cookies are disabled. As a consequence, these cookies do not fall under the exemption defined in CRITERION A or B.

However, the Working Party considers that first party analytics cookies are not likely to create a privacy risk when they are strictly limited to first party aggregated statistical purposes and when they are used by websites that already provide clear information about these cookies in their privacy policy as well as adequate privacy safeguards. Such safeguards are expected to include a user friendly mechanism to opt-out from any data collection and comprehensive anonymization mechanisms that are applied to other collected identifiable information such as IP addresses. !

[5] http://www.w3.org/TR/tracking-compliance/

Deswegen war der § 15 Abs. 3 TMG von Brüssel nicht bemängelt worden !!!

In this regard, should article 5.3 of the Directive 2002/58/EC be re-visited in the future, the European legislator might appropriately add a third exemption criterion to consent for cookies that are strictly limited to first party anonymized and aggregated statistical purposes. !

First party analytics should be clearly distinguished from third party analytics, which use a common third party cookie to collect navigation information related to users across distinct websites, and which pose a substantially greater risk to privacy.

5 Summary and guidelines

This analysis has shown that the following cookies can be exempted from informed consent under certain conditions if they are not used for additional purposes: !

1) User input cookies (session-id), for the duration of a session or persistent cookies limited to a few hours in some cases.

2) Authentication cookies, used for authenticated services, for the duration of a session.

3) User centric security cookies, used to detect authentication abuses, for a limited persistent duration.

4) Multimedia content player session cookies, such as flash player cookies, for the duration of a session.

5) Load balancing session cookies, for the duration of session.

6) UI customization persistent cookies, for the duration of a session (or slightly more).

7) Third party social plug-in content sharing cookies, for logged in members of a social network. Insofern "session"-Cookie, als dass es gelöscht wird, wenn man sich ausloggt.

Having regard to social networks, the working party notes however that the use of third party social plug-in cookies for other purposes than to provide a functionality explicitly requested by their own members requires consent, notably if these purposes involve tracking users across websites.

The working party recalls that third party advertising cookies cannot be exempted from consent, and further clarifies that consent would also be needed for operational purposes related to third party advertising such as frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging. While some operational purposes might certainly distinguish one user from another, in principle these purposes do not justify the use of unique identifiers. This point is of particular relevance in the context of the current discussions regarding the implementation of the Do Not Track standard in Europe.

This analysis also shows that first party analytics cookies are not exempt from consent but pose limited privacy risks, provided reasonable safeguards are in place, including adequate information, the ability to opt-out easily and comprehensive anonymisation mechanisms.

Some primary guidelines can be drawn from the analysis and the cookie use scenarios presented in this opinion:

1) When applying CRITERION B, it is important to examine what is strictly necessary from the point of view of the user, not the service provider.

2) If a cookie is used for several purposes, it can only benefit from an exemption to informed consent if each distinct purpose individually benefits from such an exemption.

3) First party session cookies are far more likely to be exempted from consent than third party persistent cookies. However the purpose of the cookie should always be the basis for evaluating if the exemption can be successfully applied rather than a technical feature of the cookie.

Ultimately, to decide if a cookie is exempt from the principle of informed consent it is important to verify carefully if it fulfils one of the two exemption criteria defined in Article 5.3 as modified by Directive 2009/136/EC. After a careful examination, if substantial doubts remain on whether or not an exemption criterion applies, website operators should closely examine if there is not in practice an opportunity to gain consent from users in a simple unobtrusive way, thus avoiding any legal uncertainty.

Done at Brussels, on 7th June 2012

For the Working Party
The Chairman
Jacob KOHNSTAMM