CONSENT

Working Paper 03/2017

IAB Europe
GDPR Implementation Working Group

Version 1.1

7 September 2018

About IAB Europe

IAB Europe is the voice of digital business and the leading European-level industry association for the interactive advertising ecosystem. Its mission is to promote the development of this innovative sector by shaping the regulatory environment, investing in research and education, and developing and facilitating the uptake of business standards.

About the GDPR Implementation Group

IAB Europe's GDPR Implementation Group brings together leading experts from across the digital media and advertising industries to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the sector. The GDPR Implementation Group is a member-driven forum for discussion and thought leadership. Its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

Acknowledgements

This Working Paper on consent under the General Data Protection Regulationhas been prepared by the members of the IAB Europe GDPR Implementation Group under the leadership of Alice Lincoln, Vice President – Data Policy & Governance at *MediaMath*.

Contacts

Townsend Feehan (feehan@iabeurope.eu)

CEO, IAB Europe

Matthias Matthiesen (matthiesen@iabeurope.eu)

Director, Privacy & Public Policy, IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)

Manager, Privacy & Public Policy, IAB Europe

Contents

Executive Summary

- Consent is one of six legal bases for the processing of personal data under the GDPR. The choice of which legal basis to use to justify the processing of personal data requires a context-specific analysis. One important contextual factor is other laws, such as the ePrivacy Directive, which require consent for the storing of information or accessing of information stored on end-user devices, as well as the proposed ePrivacy Regulation which will replace national laws.
- When obtaining consent, it is important that the right information is displayed to the data subject, including details such as the purposes of data processing, the types of data which will be processed, the responsible data controllers, and more. As this amounts to a lot of information, we recommend making use of a layered approach where key information is provided first, with a link to more detailed information.
- Private companies are allowed to make access to their services conditional upon the consent of data subjects. The GDPR provides that account has to be taken of this when determining whether consent has been freely given, but does not prohibit the practice. The ePrivacy Directive similarly explains that data subjects may be denied the use of a service if they do not consent to the placing of cookies.
- Consent has to be granular in terms of the purposes for which the data subject consents to processing. Publishers may decide to request for consent to all purposes together, or for individual purposes. In that case, they should make sure that where those purposes are reliant on another, consent for those purposes is tied together.
- Consent can be specific to a service, or 'global', the latter referring to a situation where consent is valid across different websites and services for the same controller. It is up to publishers and their partners to determine what they prefer to use. Consent can be obtained by first parties on behalf of their third parties. While the GDPR does not provide a time limit for the validity of consent, companies should be aware that there may be other laws which require this. It may therefore be necessary to review and refresh a user's consent at appropriate intervals.
- Companies, especially data controllers, should keep records of consent. IAB Europe recommends the adoption of an automated mechanism that communicates relevant information through the digital advertising supply chain.
- Consent must be as easy to withdraw as it is to give, but processing which takes place before the withdrawal remains legitimate. Data collected before the withdrawal of consent cannot be processed after such withdrawal, unless there is an alternative legal ground for processing that data.
- First parties are in the best position to provide users with information and obtain consent, and therefore the responsibility often falls on them to make the necessary disclosures and to obtain consent. Third parties are nonetheless responsible for ensuring that consent is validly obtained on their behalf.
- Many current approaches to getting consent (through banners) will not be sufficient for proving that users have made an affirmative action to indicate their consent. Data

processing cannot occur before the user has made such an affirmative action to indicate their consent.

- IAB Europe's GDPR Implementation Group has developed a technical standard to facilitate the exchange of information between first and third parties which is necessary to prove that consent has been given, and to pass this information along the digital advertising supply chain.

Overview

On 27 April 2016, the European Union adopted the General Data Protection Regulation ("GDPR").[1] The GDPR became directly applicable law in the European Union ("EU") and European Economic Area ("EEA") on 25 May 2018, replacing previous national data protection laws.

The GDPR regulates the processing of personal data, defined broadly as any information that relates to an identified or identifiable natural person, which includes online and device identifiers that can be used to single out a natural person.[2] For processing of personal data to be lawful, it must be justified by at least one of six legal grounds for processing.

This document has been prepared by members of the IAB Europe GDPR Implementation Group to provide guidance to companies that choose, or are required by law, to process personal data based on a data subject's consent.

Processing Personal Data with Consent

Consent Under the GDPR

Consent under the GDPR is a much more robust concept than consent under the existing European Data Protection Directive. Unlike the European Data Protection Directive, the GDPR is very explicit in its description of the requirements pertaining to consent, effectively ending certain interpretations and implementations of consent on the basis of the old law. This most notably applies to certain notions of "implied consent" that considered a user to had consented to a request by virtue of not taking any action, as under the GDPR consent requires an affirmative act.

Consent is defined in Article 4(11) GDPR:

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at http://eur-lex.europa.eu/eli/reg/2016/679/oj/.

[2] See IAB Europe paper on the definition of personal data, available at https://www.iabeurope.eu/policy/gig-working-paper-on-the-definition-of-personal-data/.

> "'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[3]

In addition to (ordinary) consent as defined above, the GDPR introduces a second type of consent, too: explicit consent. Explicit consent is not defined in the GDPR, but is generally interpreted as a higher standard with some stricter requirements, such as requiring a more explicit affirmative act or statement that the data subject must take to convey explicit consent. In situations where consent applies, the GDPR usually requires ordinary consent, with explicit consent being more limited in its application.

When is consent required?

Organisations which wish to process personal data need to justify its processing under EU law. The GDPR offers six legal grounds to achieve this, of which at least one must apply.[4] The data subject's consent to the processing of personal data relating to him or her is one such legal ground. Notably, all legal grounds are equal and no single legal ground enjoys an elevated status. A company's choice of the most appropriate legal basis for the processing of personal data should be subject to a context-specific assessment, taking into account all relevant rules found in the GDPR and other laws.

The GDPR recognizes certain special categories of personal data that cannot be processed unless more stringent requirements contained in Article 9(2) are met, such as the data subject's explicit consent. Moreover, certain types of personal data processing are subject to more stringent requirements as well, such as transfers of personal data outside of the territory of the EU who have not been deemed as offering an adequate level of protection,[5] or decisions based solely on automated processing that produce legal or similarly significant effects. Companies wishing to process special categories of personal data, or engage in specific regulated processing activities, should be sure to comply with the more stringent processing requirements.

In addition, other laws may impact the decision as to which legal ground for processing is most appropriate or required. Notably, the so-called "cookie provision" of the ePrivacy Directive states:

> "[…] that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the

[3] Article 4(11) GDPR.

[4] See Article 6 GDPR: The GDPR permits processing where (a) the data subject has given consent to the processing; (b) the processing is necessary for performance of a contract or to enter into a contract; (c) processing is necessary for compliance with a legal obligation; (d) processing is necessary to protect the vital interests of the data subject or another natural person; (e) processing is necessary for carrying out a task in the public interest; (f) processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests and fundamental rights of the data subject.

[5] Note that other methods for transferring data outside of the European Union exist, too. See, for example "Data transfers outside the EU" by the European Commission, available at http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm.

subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with [the GDPR],[6] inter alia, about the purposes of the processing."

Article 95 GDPR on the relationship of the GDPR with the ePrivacy Directive establishes that the ePrivacy Directive's more specific rules prevail over rules of the GDPR. Therefore, companies storing information (e.g., in cookies) or accessing information (e.g., device identifiers, such as AAID, IDFA, or statistical identifiers generated through fingerprinting techniques) should be sure to consider the relevant national laws implementing the ePrivacy Directive when choosing the appropriate legitimate basis for their data processing.[7] Companies should also stay up to date on the ongoing discussions for an ePrivacy Regulation, which is expected to replace and change the rules of the existing ePrivacy Directive sometime after May 2018. While a directive (such as the ePrivacy Directive) generally needs to be transposed into national law by individual member states before it creates legal obligations for companies, a regulation (such as the GDPR, and the proposed ePrivacy Regulation) is directly applicable in the entirety of the EU without the need for transposition into national law by member states.

Disclosing the Right Information for a Consent Request

The GDPR stipulates that the data subject must be informed at least of the identity of the controller and the purposes for which the personal data are to be processed.[8] Moreover, consent must be intelligible, referring clearly and precisely to the scope and the consequences of the processing. According to the Article 29 Working Party "[t]his means in practice that consent by the data subject (must be) based upon an appreciation and understanding of the facts and implications of an action. The individual concerned must be given, in a clear and understandable manner, accurate and full information of all relevant issues".[9]

Therefore, in order to be valid, consent requests and information must (1) be provided prominently and separately from other information, such as terms and conditions;[10] (2) be presented in plain language that is easy to understand;[11] (3) describe the nature of the personal data processed (e.g. random identifiers, browsing data);[12] (4) describe the purpose of – or reason for – the processing;[13] (5) explain the consequences (if any) of the processing;[14] (6) list the controller or various controllers

[6] The ePrivacy Directive relies on the definition of consent found in the Data Protection Directive Article 94(2). GDPR stipulates that all references to the Data Protection Directive "shall be construed as references to [the GDPR]". As a result, the consent requirement under the ePrivacy Directive shall be that of the GDPR.
[7] For an overview of national "cookie" rules see IAB Europe ePrivacy Directive Implementation Center, available at http://www.iabeurope.eu/eucookielaws.
[8] Recital 42 GDPR.
[9] Ibid.
[10] Article 7(2) GDPR; Recital 42 GDPR.
[11] Article 7(2) GDPR; Recital 42 GDPR.
[12] Article 29 Working Party Opinion 187 on the definition of consent, p. 19, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
[13] Recital 42 GDPR.
[14] Article 29 Working Party Opinion 187 on the definition of consent, p. 19, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

that will be relying on the consent to process personal data – individually by name;[15] (7) inform users of their right to withdraw consent, as well as how to do so;[16] and (8) educate users about the consequences of not consenting to the processing, e.g. a reduced user experience or being prevented to use a site or service.[17]

The GDPR does not require that consent requests list the names of processors which will process the data on behalf of a controller. The processor can do so on the basis of the consent granted to its controller.

Because of the extensive information disclosures required by the GDPR, which will make it impossible or impractical to provide all details at the same time, IAB Europe recommends making use of a "layered approach" for disclosing all relevant information. According to the ICO, the UK's data protection authority, layered approaches work "very well" in an online context, such as the digital advertising context.

> "A layered approach can be useful as it allows you to provide the key privacy information immediately and have more detailed information available elsewhere for those that want it. This is used where there is not enough space to provide more detail or if you need to explain a particularly complicated information system to people.
>
> It usually consists of a short notice containing the key information, such as the identity of the organisation and the way you will use the personal information. It may contain links that expand each section to its full version, or a single link to a second, longer notice which provides more detailed information. This can, in turn, contain links to further material that explains specific issues, such as the circumstances in which information may be disclosed to the police."[18]

This document provides practical suggestions below in the section entitled "Obtaining Valid Affirmative Consent in Practice".

Consent as a Condition for Accessing a Service

When determining whether consent is freely given, the GDPR mandates taking into "utmost account"[19] whether, amongst others, the provision of a service is conditional on consent to processing not necessary for provision of the service. Recital 43 describes this requirement as:

[15] Recital 42 GDPR.
[16] Article 7(3) GDPR.
[17] Article 29 Working Party Opinion 187 on the definition of consent, p. 19, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
[18] *See* Information Commissioner's Office code of practice on privacy notices, transparency and control on where privacy information should be delivered to individuals, available at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/where-should-you-deliver-privacy-information-to-individuals/ ((accessed 20/11/2017, 12:10 CET)
[19] Article 7(4) GDPR.

> "Consent is presumed not to be freely given if […] the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

Importantly, the GDPR does not establish a prohibition on making access to a service conditional on consent, although it requires a context specific assessment.

The ePrivacy Directive clarifies that access to "website content may still be made conditional on the well-informed acceptance of cookies"[20] and use of similar tracking technologies. As a result, digital services, such as websites or apps are generally permitted to require users to consent to the collection their personal data through cookies or similar technologies before allowing them to use a service.

While the Article 29 Working Party recommends that companies do not make access conditional on consent, it recognises that access to privately-owned services can be made conditional on acceptance to cookies and that in certain member states the law explicitly provides for that possibility, such as in Sweden.[21] However, rules may be less permissive for publicly-owned services.[22] The Danish Business Authority takes the view that it is "not unlawful to have solutions that reject users who do not want to accept the use of cookies,"[23] and that "refusal of cookies might imply that the user's only option is to leave the site."[24] Again, the regulator took the view that different rules might apply to publicly funded services. The Dutch Consumer and Markets Authority, which enforces the ePrivacy Directive, also states that websites are not required to grant access to users to their website who do not accept cookies, and are therefore permitted to make access conditional upon consent to cookies. The regulator further considers that website owners may have other interests which would allow them to choose to make access conditional on consent. Including that the way a user "pays" for receiving access to a service is receiving targeted advertisements. [25]

IAB Europe's position is that, when read together, the GDPR and ePrivacy Directive clearly allow private businesses to deny access to users who do not consent to data processing. Publishers are free to decide themselves which methods of obtaining consent fit best with their respective business models, including whether access to their service should be conditional on such consent and/or whether user experiences should vary depending on the user's choices.

---

[20] Recital 25 ePD.
[21] Article 29 Working Party Working Document 02/2013 providing guidance on obtaining consent for cookies, p. 5, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
[22] Ibid., p. 6.
[23] Erhvervsstyrelsen, Guidelines on Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-User Terminal Equipment ("Cookie Order"), p. 20, available at https://erhvervsstyrelsen.dk/sites/default/files/media/engelsk-vejledning-cookiebekendtgorelse.pdf.
[24] Ibid.
[25] Autoriteit Consument en Markt (ACM), Frequently asked questions about the Dutch cookie act October 2016, p. 12, available at https://www.acm.nl/sites/default/files/old_publication/publicaties/11917_veelgestelde-vragen-cookiebepaling-oktober-2016-engels-new.pdf.

Granularity of Consent

In order for consent to be informed, the purposes for which data are processed must be fully disclosed.[26] In addition, for consent to be freely given the data subject should be able to consent separately to different personal data processing operations if such granularity is "appropriate" in the individual case.[27] This means that, where appropriate, a controller could request and obtain consent for a number of purposes *en bloc* without offering the data subject the possibility to agree only to a subset of those purposes. In other cases, it may be appropriate for a controller to allow a user to consent to different purposes separately, enabling them to make more granular choices. It is ultimately up to the publishers to determine the appropriateness of granularity, based on their expertise of how their services and controls work, about which purposes are appropriate conditions for accessing a service or which purposes are required for a given user experience. Where one purpose is dependent on another purpose, it should not be possible to consent to the former without also consenting to the latter. For example, interest-based advertising might rely on analytics to measure the effectiveness of an advertisement. Therefore, a user consenting to interest-based advertising also needs to consent to analytics as the former depends on the latter.

Scope of Consent

Consent can be obtained by a first party on behalf of themselves and their partners (and partners' partners) on a "service-specific" or "global" basis. "Service-specific" consent describes a consent state for a given controller that is limited in scope to a single site or service, whereas "global" consent describes a consent state for a given controller without limitations about where that consent can be leveraged.

The Article 29 Working Party has endorsed the principle of global consent on the basis that it will provide a better user experience. Specifically, in their view, for an average user, the number of consent requests will decrease over time as the user navigates and expresses their consent on the internet, because:

> "[…] if a third party ad network on a website receives consent for an OBA cookie, this consent will not only be valid on other pages of the same website, but also for other websites that share the same OBA network."[28]

Companies will want to make sure that they know what type of consent, i.e. global or service-specific, they have obtained via a different entity (i.e. first party) as that determines the scope of their permitted data collection and processing. To that end, third parties who rely on consent obtained on their behalf by first parties should consider contractual clauses and/or other

[26] Recital 42 GDPR.
[27] Recital 43 GDPR.
[28] Article 29 Working Party Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioral Advertising WP 188, pp. 10-11, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf

mechanisms, including technical mechanisms, that surface the scope (e.g. “global”) as well as the purposes (e.g. “interest-based advertising”) sought by the third party.

The GDPR does not contain a time limit for the validity of consent. Accordingly, consent is valid as long as the processing of personal data is necessary to fulfil its purpose or until the data subject withdraws consent. In any case, the decision of how long consent should be valid for should be underpinned by a context-specific assessment taking into account all relevant factors, such as the nature and duration of the processing. The Article 29 Working Party recommends that consent should be reviewed and refreshed in appropriate intervals as a matter of good practice. There might also be other laws, regulations or rules, that are relevant in determining how often consent needs to be refreshed. For example, the French data protection authority considers that tracking cookies may only be stored for 13 months before they should expire, which would require controllers to obtain consent from a user for storing or accessing cookies on their device at least every 13 months.[29] Companies should therefore be sure to consider all relevant factors when determining how often to refresh consent – or if at all. However, a controller may need to request consent from a given user sooner if the controller cannot verify that the user has already given it, in order to ensure that no processing takes place without valid consent.

Recording Consent for Demonstration of Compliance

The GDPR requires that controllers be “able to demonstrate that the data subject has consented to processing of his or her personal data.”[30] This means that all controllers (first parties, and third parties alike) must keep records of what the individual has consented to, including the language presented in the consent mechanism, and when and how they consented.

In situations where a controller is processing data on the basis of consent obtained by another entity, the controller should obtain and keep a record demonstrating that consent has been given to be able to comply with this obligation. For this reason, it is essential that the user’s consent be propagated from the first party to all relevant third parties so that each party can maintain a documented audit trail. IAB Europe recommends adoption of an automated mechanism that communicates relevant information through the digital advertising supply chain.

Such records should include at least:

- The date and time at which the user has granted consent
- The URL on which the user has granted consent
- The action that the user took to signify consent
- The purposes for which the user has granted consent
- The controller or controllers for which the user has granted consent
- The information that has been presented to the user before they granted consent
- An identifier enabling the controller to tie the individual consent to the relevant user

[29] CNIL, Cookies & traceurs: que dit la loi? (Cookies & trackers: what does the law say?), available in French at, https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi/. (accessed 15/09/2017, 10:50 CEST)
[30] Article 7(1) GDPR.

The Right to Withdraw Consent

Data subjects also have the right to withdraw their consent at any time, which must be as easy to do as it was to give it in the first place.[31] When a data subject withdraws his or her consent, the lawfulness of processing that has taken place on the basis of that consent before its withdrawal is not affected.[32] However, any future lawful processing of data already collected or to be collected in the future will require an alternative legal ground for processing.

In addition, where the user withdraws their consent for a certain data processing activity, and there is no other legal basis for continuing the processing, the user has the right to request erasure (or anonymisation) of personal data concerning him or her.[33]

When a controller obtains such a request to erase data, it must honor the request "without undue delay", unless the data are necessary (1) for exercising the right to freedom of expression; (2) for compliance with a legal obligation; (3) for reasons of public interest in public health; (4) for public interest, scientific or historical research and statistical purposes; or (5) for the establishment, exercise or defense of legal claims.[34]

Lastly, controllers who have disclosed the data to other controllers must take "reasonable steps" to pass on to those other controllers the user's erasure request.[35]

Responsibilities of First and Third Parties[36]

First parties are best positioned to (and often the only entities in the digital advertising supply chain that can) provide information to users and obtain their consent. It follows that first parties must make the necessary disclosures about data processing that occurs as a result of a user accessing their site, app or other service and request user consent for both the data processing they are responsible for, as well as the data processing undertaken by third parties.

However, even where third parties are unable to make disclosures and to obtain consent themselves, they could be liable if the information disclosures made, and consents obtained, by their first party partners are not legally valid and result in the third party's non-compliance with the

[31] Article 7(3) GDPR.
[32] Article 7(3) GDPR.
[33] Article 17(1)(b) GDPR.
[34] Article 17(3) GDPR.
[35] Article 19 GDPR.
[36] According to the Article 29 Working Party a third party is "a data controller that is distinct from the one that operates the [service] accessed by the user" at any given time. Conversely, a first party is a data controller that operates the service accessed by the user. This classification may be different from purely technical classifications of first and third parties. *See* Article 29 Working Party Opinion on Cookie Consent Exemption, pps. 4-5, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

law.[37] It is therefore extremely important that the digital advertising ecosystem cooperates closely to meet individual companies' obligations for making appropriate disclosures and obtaining valid consent under the GDPR.

Statements or Conduct Qualifying as Affirmative Consent

The Article 29 Working Party has stated that "[t]here is in principle no limits as to the form consent can take [other than that] it should be an indication."[38] Recital 32 GDPR provides examples of what is, and is not, meant by a "clear affirmative action":

> "This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent."[39]

As a result of the implementation of the ePrivacy Directive, obtaining consent for the collection of personal data through cookies for the purpose of online advertising and analytics has – in many EU Member States – centred around the idea "consent banners", a banner placed at the top or bottom of the page containing disclosures with a consent request.

While consent banners can still be a helpful tool for disclosing information and obtaining valid consent under the GDPR, many current implementations of so-called implied consent will require changes in practice as it will no longer be possible to infer consent from the mere fact that a user has not made use of a possibility to refuse consent.

This is because, unlike under the Data Protection Directive, the GDPR is clear that processing any personal data must not start *before* the action qualifying as consent has taken place.

As processing with user consent, such as the collection of data through cookies, must not start before a positive act, first parties might want to display an interstitial site requesting consent – a "consent wall" – instead. This would guarantees that users have read and consented to the processing activities required by the service before using it. While consent could also still be expressed through the action of further using a service after the appropriate disclosures have been made, for example via a "consent banner", it is important that no data collection and processing takes place before a positive action unambiguously conveying consent has been detected:

> "The process by which users could signify their consent for cookies would be through a positive action or other active behaviour, provided they have been fully informed of what

[37] The French data protection authority concluded that publishers alone cannot be held responsible for third party cookies because they originate from a different company who is responsible for the processing, and as a result required to comply with data protection law. *See* CNIL, Cookies: la CNIL etend ses controles au-dela des editeurs de sites (Cookies: the CNIL extends its controls beyond site operators), available at https://www.cnil.fr/fr/cookies-la-cnil-etend-ses-controles-au-dela-des-editeurs-de-sites/ (accessed 15/09/2017, 10:50 CEST).

[38] Article 29 Working Party Opinion 187 on the definition of consent, p. 11, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

[39] Recital 32 GDPR.

> that action represents. Therefore the users may signify their consent, either by clicking on a button or link or by ticking a box in or close to the space where information is presented (if the action is taken in conjunction with provided information on the use of cookies) or by any other active behaviour from which a website operator can unambiguously conclude it means specific and informed consent."[40]

The Article 29 Working Party defines "active behaviour" as a user action "based on a traceable user-client request towards the website."[41] Moreover, the Article 29 Working Party considers that "[t]he user action must be such that, taken in conjunction with the provided information on the use of cookies, it can reasonably be interpreted as indication of his/her wishes."[42] The French data protection authority in addition states that consent "can be expressed by scrolling the web page visited."[43]

Obtaining Valid Affirmative Consent in Practice

IAB Europe's Transparency & Consent Framework (Framework) has a simple objective to help all parties in the digital advertising chain ensure that they comply with the EU's General Data Protection Regulation and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies.

The Framework is particularly relevant for "first-parties", such as publishers and other suppliers of online services, who work with "third-parties" for data-driven service. Using the Framework, first-parties can enable third-parties to process user data on one of the legal bases of the regulation. The Framework standardises the presentation to users' third-party data processing requests that require "informed" consent for data processing. The Framework enables "signaling" of user choice across the advertising supply chain. It is open-source, not-for-profit with consensus-based industry governance led by IAB Europe with significant support from industry parties and the IAB Tech Lab, which provides technical management of the open-source specifications and version control.[44]

Legacy Consent: Validity of Consent Collected Prior to the GDPR

Legacy consent, i.e. consent obtained before the date of application of the GDPR, remains valid provided that consent has been obtained in a manner compliant with the GDPR.[45] However, where legacy consent does not meet the high standard for consent of the GDPR, that consent will lose its

[40] Article 29 Working Party Working Document 02/2013 providing guidance on obtaining consent for cookies, p. 4, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf.
[41] Ibid.
[42] Ibid.
[43] CNIL, Cookies: la CNIL etend ses controles au-dela des editeurs de sites (Cookies: the CNIL extends its controls beyond site operators), available at https://www.cnil.fr/fr/cookies-la-cnil-etend-ses-controles-au-dela-des-editeurs-de-sites/ (accessed 15/09/2017, 10:50 CEST).
[44] You can learn more about the Transparency and Consent Framework at http://advertisingconsent.eu.
[45] Recital 171 GDPR.

validity for continued processing once the GDPR becomes applicable. In such cases the controller must find an alternative legal basis for processing, obtain new consent in line with the GDPR, or cease the processing activity in question. Most companies in the advertising ecosystem will likely need to obtain new consents in line with the rules of the GDPR.

Consent of Children Below the Age of 16

Where an internet service is offered directly to a child, consent is only a legal ground for processing if the child is at least 16 years old; where the child is younger, parental consent is required. Member states may adopt legislation to lower the threshold to provided that such lower age is not below 13 years. Where parental consent is required controllers must also take reasonable steps to validate such consent.

About the IAB Europe GDPR Implementation Working Group

IAB Europe's GDPR Implementation Working Group brings together leading experts from across the digital advertising industry to discuss the European Union's new data protection law, share best practices, and agree on common interpretations and industry positioning on the most important issues for the digital advertising sector.

The GDPR Implementation Working Group is a member-driven forum for discussion and thought leadership, its important contribution to the digital advertising industry's GDPR compliance efforts is only possible thanks to the work and leadership of its many participating members.

For more information please contact:

Townsend Feehan (feehan@iabeurope.eu)
CEO
IAB Europe

Matthias Matthiesen (matthiesen@iabeurope.eu)
Director, Privacy & Public Policy
IAB Europe

Chris Hartsuiker (hartsuiker@iabeurope.eu)
Manager, Privacy & Public Policy
IAB Europe