Deliberation 2020-092 of September 17, 2020Commission Nationale de l'Informatique et des LibertésNature of the deliberation: RecommendationLegal status: In force Date of publication on Légifrance: Tuesday, October 06, 2020NOR: CNIL2026188XDeliberation No. 2020-092 of September 17, 2020 adopting a recommendation proposing practical methods of compliance in the event of the use of "cookies and other tracers"The National Commission for Computing and Liberties,

Having regard to Convention No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC;

Having regard to Directive 2002/58/EC of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, amended by Directive 2009/136/EC of November 25, 2009;

Having regard to Directive 2008/63/EC of June 20, 2008 relating to competition in the markets for telecommunications terminal equipment, in particular its article 1;

Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms, in particular its articles 8-I-2°-b and 82;

Having regard to decree n° 2019-536 of May 29, 2019 as amended, taken for the application of law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to Guidelines 5/2020 on consent within the meaning of Regulation (EU) 2016/679 adopted on May 4, 2020 by the European Data Protection Board (EDPS);

Having regard to deliberation no. 2020-091 of September 17, 2020 adopting guidelines relating to the application of article 82 of the law of January 6, 1978 as amended to read or write operations in a user's terminal (in particular to cookies and other tracers);

After having heard Mr. François PELLEGRINI, commissioner, in his report, and Mr. Benjamin TOUZANNE, government commissioner, in his observations, Makes the following observations:

On September 17, 2020, the National Commission for Computing and Liberties (hereinafter the Commission) adopted guidelines relating to the application of article 82 of the law of January 6, 1978 as amended (hereinafter the Data Protection

Act). The main purpose of these guidelines is to recall and explain the law applicable to the operations of reading and/or writing information (hereafter the tracers) in the electronic communications terminal equipment of the subscriber or the user (hereinafter users).

The Commission wished to supplement its guidelines with this recommendation in order to propose practical procedures for obtaining consent in accordance with the applicable rules.

This recommendation, and in particular the examples proposed therein, is neither prescriptive nor exhaustive and has the sole objective of helping the professionals concerned in their compliance process. Other methods of obtaining consent may be used by professionals, provided that they make it possible to obtain consent in accordance with the texts in force.

This recommendation was drawn up following consultation with representatives of the professions concerned by digital advertising as well as with representatives of civil society. It was also the subject of a public consultation from January 14 to February 25, 2020.Article 1 - Scope of the recommendation.1.1. Actors concerned

This recommendation concerns all organizations that use tracers, as defined in the guidelines of September 17, 2020.1.2. Affected environments

This recommendation takes particular account of the configurations specific to web environments and mobile applications. Practical examples can, however, inspire and guide the development of interfaces in other contexts where the consent provided for in Article 82 of the Data Protection Act is required: connected television, video game console, voice assistant, communicating objects , connected vehicle, etc.

The recommendation concerns both environments in which users are authenticated (sometimes called logged in universes) and universes in which they are not (unlogged in universes). Indeed, the fact that users are authenticated does not dispense with obtaining their consent in accordance with Article 82 of the Data Protection Act, when tracers subject to consent are used.

Article 2 - Information, consent and refusal. As recalled by the guidelines of September 17, 2020, when none of the exceptions provided for in Article 82 of the Data Protection Act is applicable, users must, on the one hand, receive information in accordance with this article, supplemented, where applicable, by the requirements of the GDPR, and, on the other hand, to be informed of the consequences of their choice.

Within this guideline, the lack of user consent is referred to as opt-out. Any inaction or action by users other than a positive act signifying their consent must be interpreted as a refusal to consent; in this case, no read or write operation subject to consent

can legally take place.

In general, in order to be understandable and not to mislead users, the Commission recommends that the organizations concerned ensure that users take full measure of the options available to them, in particular through the design chosen and the information delivered.

Furthermore, the Commission encourages the development of standardized interfaces, operating in the same way and using a uniform vocabulary, so as to facilitate the understanding of users when browsing mobile sites or applications.2.1. Information on the purposes of tracers

As recalled in the guidelines, the purposes of the trackers must be presented to users before they are offered the opportunity to consent or refuse. They must be formulated in an intelligible way, in a suitable language and sufficiently clear to allow users to understand precisely what they are consenting to.

In order to facilitate reading, the Commission recommends that each purpose be highlighted in a short and highlighted title, accompanied by a brief description. Examples for complying with the applicable rules are presented below, in a non-exhaustive manner:

- if the tracker(s) are used to display personalized advertising, this purpose can be described as follows: Personalized advertising: [name of the site / application] [and third party companies / our partners] uses / use trackers to display personalized advertising based on your browsing and your profile;
- if the tracker(s) are only used to measure the audience for the advertising displayed, without selecting it on the basis of personal data, the controller may use the following wording: Non-personalized advertising: [site name / of the application] [and third party companies / our partners] use / use trackers for the purpose of measuring the audience of advertising [on the site or the application], without profiling you;
- if the advertising is adapted according to precise geolocation, this purpose can be described as follows: Geolocated advertising: [name of the site / application] [and third party companies / our partners] uses / uses trackers to send you advertising based on your location;
- if trackers are used to personalize editorial content or delivered products and services displayed by the publisher, the following wordings may be displayed: Content personalization: Our site/application [and third-party companies] use/use trackers to customize editorial content [on our site/app] based on your usage, or Our site/app [and third-party companies]

use/use trackers to customize the display of our products and services based on those you have previously viewed [on our site/app]);

- if tracers are used to share data on social networks, their purpose can be described as follows: Sharing on social networks: Our site / application uses tracers to allow you to share content on social networks or platforms present [on our site / application]. If the publisher has chosen to set up a mechanism allowing these tracers to be triggered only when the users actually wish to share data with the social networks concerned (and when they interact with the functionality or the button allowing this interaction), the information and collection of consent could appear when users decide to trigger said sharing functionality.

The Commission also recommends including, in addition to the list of purposes presented on the first screen, a more detailed description of these purposes, easily accessible from the consent collection interface. This information can, for example, be displayed under a drop-down button that the Internet user can activate directly at the first level of information. It can also be made available by clicking on a hypertext link present at the first level of information.

The content of this additional information may, for example, specify that the display of the advertisement encompasses different technical operations contributing to the same purpose. These also include display capping (sometimes called ad capping, consisting of not presenting a user with the same advertisement too repetitively), the fight against click fraud (detection of publishers claiming to achieve an audience advertising higher than reality), the billing of the display service, the measurement of targets with more appetite for advertising to better understand the audience, etc.

Finally, in order to increase transparency, a data controller may also specify the categories of data collected by associating them with the purposes they enable to be achieved.2.2. Information on the scope of consent

When tracers subject to consent, deposited by entities other than the publisher of the site or the mobile application, allow monitoring of the user's navigation beyond the site or the mobile application where these are initially filed, the Commission strongly recommends that consent be collected on each of the sites or applications concerned by this navigation tracking, in order to guarantee that the user is fully aware of the scope of his consent.2.3. Information concerning the identity of the controller(s)

Users must be able to find out the identity of all the controllers of the processing, including the joint controllers, before giving their consent or refusing. Thus, as explained in the guidelines of September 17, 2020, the exhaustive and regularly updated list

of data controllers must be made available to users when obtaining their consent.

In practice, in order to reconcile the requirements for clarity and conciseness of information with the need to identify all of the data controller(s), specific information on these entities (identity, link to their personal data processing policy staff), regularly updated, can for example be provided at a second level of information. They can thus be made available from the first level via, for example, a hypertext link or a button accessible from this level. The Commission further recommends using a descriptive name and using clear terms, such as list of companies using trackers on our site / application.

Finally, the Commission recommends that such a list should also be made available to users on a permanent basis, in a place easily accessible at any time on the website or mobile application. Thus, the mechanism for viewing the updated list of data controllers should preferably be placed in areas of the screen that attract the attention of users or in areas where they expect to find it, while throughout their journey. For example, the publisher of a website can provide users with a configuration module accessible on all the pages of the site by means of a static cookie icon that is always visible or a hypertext link located at the bottom or top of page.

In order to increase the reading of the information by the users, the number of managers of the treatment(s) involved could be indicated at the first level of information. Similarly, the role of those responsible for the processing(s) could be highlighted by grouping them into categories, which would be defined according to their activity and the purpose of the tracers used.2.4. The expression of consent or refusalAs regards the unequivocal nature of consent

Consent must be manifested by a clear positive act by users, meeting the conditions set by the GDPR, interpreted by the Commission in its guidelines of September 17, 2020.

The Commission considers that a request for consent made by means of checkboxes, unchecked by default, is easily understandable by users. The data controller may also use switches (sliders), deactivated by default, if the choice expressed by the users is easily identifiable. The Commission recommends to be careful that the information accompanying each actionable element allowing to express a consent or a refusal is easily understandable and does not require effort of concentration or interpretation on the part of the user. Thus, it is particularly recommended to ensure that it is not written in such a way that a quick or inattentive reading could lead to believe that the selected option produces the opposite of what users thought they were choosing. concerning the free nature of the consent

Consent can only be valid if users are able to freely exercise their choice.

In order to ensure the free nature of the consent given, the Commission recommends asking users for their consent independently and specifically for each distinct purpose.

However, the Commission considers that this does not preclude the possibility of offering users consent in a global manner to a set of purposes, subject to prior presentation to users of all the purposes pursued.

In this respect, the Commission stresses that it is possible to offer global acceptance and refusal buttons at the first level of information stage, for example by presenting buttons entitled accept all and refuse all , I authorize and I do not authorize, I accept everything and I accept nothing and allowing to consent or refuse, in a single action, to several purposes.

To allow people to choose purpose by purpose, it is possible to include a button, on the same level of information as the links or buttons allowing to accept everything and refuse everything, allowing access to the choice purpose by purpose. For example, a personalize my choices or decide by purpose button would clearly indicate this possibility. Users could also be offered to accept or refuse purpose by purpose directly on the first level of information. They might also be asked to click on each purpose so that a drop-down menu offers them accept or decline buttons.

In general, the Commission recommends using a descriptive and intuitive name so that users can be fully aware of the possibility of exercising a choice by purpose.

The data controller must offer users both the possibility of accepting and refusing read and/or write operations with the same degree of simplicity.

Thus, the Commission strongly recommends that the mechanism for expressing a refusal to consent to read and/or write operations be accessible on the same screen and with the same facility as the mechanism for expressing consent. Indeed, it considers that consent collection interfaces that require a single click to consent to tracking while several actions are necessary to configure a refusal to consent present, in most cases, the risk of biasing the choice of user, who wishes to be able to view the site or use the application quickly.

For example, at the stage of the first level of information, users can have the choice between two buttons presented at the same level and in the same format, on which are written respectively accept all and refuse all , authorize and prohibit , or consent and do not not consent , or any other equivalent and sufficiently clear wording. The Commission considers that this modality constitutes a simple and clear way to allow the user to express his refusal as easily as his consent.

The expression of refusal to consent may, however, result from other types of actions than that consisting of clicking on one of

the buttons described above. In any event, the Commission points out that the terms allowing users to consent or refuse must be presented in a clear and understandable manner. In particular, when the refusal can be manifested by the simple closing of the consent collection window or by the absence of interaction with it for a certain period of time, this possibility must be clearly indicated to the users on this window. Indeed, failing this, the user would be likely not to understand that these actions lead to the fact that no read or write operation subject to consent can legally take place. Appropriate design and information should allow him to fully understand the options available to him.

In order not to mislead users, the Commission recommends that data controllers ensure that the interfaces for collecting choices do not incorporate potentially misleading design practices that lead users to believe that their consent is mandatory or that visually more worth one choice than another. It is recommended to use buttons and a font of the same size, offering the same ease of reading, and highlighted in an identical way.

The Commission observes that it is, in principle, necessary to keep the choices expressed by users during their navigation on the site. Indeed, if these choices were not kept, users would be displayed a new consent request window on each page consulted, which could affect their freedom of choice.

In addition, the Commission recommends that, where refusal can be manifested by continued navigation, the message requesting consent (for example, the window or the banner) disappears after a short period of time, so as to not to interfere with the use of the site or the application and not to condition the user's browsing comfort on the expression of his consent to the tracker.

In general, the Commission recommends that the choice expressed by users, whether consent or refusal, be recorded so as not to solicit them again for a certain period of time. The retention period of these choices will be assessed on a case-by-case basis, with regard to the nature of the site or application concerned and the specificities of its audience.

Furthermore, insofar as consent may be forgotten by the persons who expressed it at a given time, the Commission recommends that data controllers renew its collection at appropriate intervals. In this case, the period of validity of the consent chosen by the controller must take into account the context, the scope of the initial consent and the expectations of users.

In view of these elements, the Commission considers, in general, that keeping these choices (both consent and refusal) for a period of 6 months constitutes good practice for publishers.Article 3 - Withdrawal and management of consent .Users who have given their consent to the use of trackers must be able to withdraw it at any time. The Commission recalls that it must be

as simple to withdraw consent as to give it.

Users must be informed in a simple and intelligible way, even before giving their consent, of the solutions available to them to withdraw it.

In practice, the Commission recommends that the solutions enabling users to withdraw their consent should be easily accessible at any time. The ease of access can be measured in particular by the time spent and the number of actions necessary to effectively withdraw consent.

The possibility of withdrawing consent may for example be offered via a link accessible at any time from the service concerned. It is recommended to use a descriptive and intuitive name such as cookie management module or manage my cookies or cookies, etc. The publisher of a website can also provide users with a configuration module accessible on all the pages of the site by means of a cookie icon , located for example at the bottom left of the screen, allowing them to access the mechanism for managing and withdrawing their consent.

In any case, the Commission recommends that the mechanism for managing and withdrawing consent be placed in an area that attracts the attention of users or in areas where they expect to find it, and that the visuals used be as explicit as possible.

Finally, for the withdrawal of consent to be effective, it may be necessary to put in place specific solutions to guarantee that the trackers previously used cannot be read or written. Article 4 - Proof of consent. processing must be able to demonstrate, at any time, that users have given their consent. To do this, mechanisms to demonstrate that users' consent has been validly obtained must be put in place.

In the event that these organizations do not themselves collect the consent of users (in particular for so-called third-party cookies), the Commission considers that such an obligation cannot be fulfilled by the mere presence of a contractual clause committing the one of the parties to obtain valid consent on behalf of the other party, insofar as such a clause does not make it possible to guarantee, in all circumstances, the existence of valid consent. In this respect, the Commission recommends that such a clause be supplemented to specify that the organization obtaining the consent must also make proof of the consent available to the other parties, so that each data controller wishing to avail himself of it can actually report.

With regard to proof of the validity of consent, the Commission recommends in particular the following non-exclusive methods:

- the different versions of the computer code used by the organization collecting the consent can be placed in escrow from a third party, or, more simply, a digest (or hash) of this code can be published in a timestamped manner on a platform. public

form, to be able to prove its authenticity a posteriori;

- a screenshot of the visual rendering displayed on a mobile or fixed terminal can be kept, in a timestamped manner, for each version of the site or of the application;

- regular audits of the consent collection mechanisms implemented by the sites or applications from which it is collected may be implemented by third parties mandated for this purpose;

- information relating to the tools implemented and their successive configurations (such as consent collection solutions, also known as CMP, for Consent Management Platform) may be stored, in a time-stamped manner, by third parties publishing these solutions.Article 5 - Tracers exempted from obtaining consent.The Commission notes that Article 82 of the Data Protection Act does not require users to be informed of the existence of read and write operations not subject to consent prior. For example, the use by a website of a language preference cookie storing only a value indicating the preferred language of the user is likely to be covered by the exemption and does not constitute processing of personal data. subject to GDPR. However, in order to ensure full and complete transparency on these operations, the Commission recommends that users are also informed of the existence of these tracers and their purposes by including, for example, a mention concerning them in the confidentiality policy. .

With regard, more specifically, to audience measurement trackers exempt from obtaining consent as described in Article 5 of the guidelines of September 17, 2020, the Commission also recommends that:

- users are informed of the implementation of these tracers, for example via the privacy policy of the site or the mobile application;

- the lifespan of the tracers is limited to a period allowing a relevant comparison of audiences over time, as is the case with a period of thirteen months, and that it is not automatically extended during new visits;

- the information collected through these tracers is kept for a maximum period of twenty-five months;

- the life and retention periods mentioned above are subject to periodic review. Article 6 - Technical measures to increase the transparency of tracers. The use of different cookies for each distinct purpose would allow users to distinguish them and to ensure that their consent is respected, but also to make read or write operations more transparent. More specifically, the Commission recommends that the tracers previously listed as being exempt from obtaining consent be used only for one and the same purpose, so that the absence of user consent has no effect on the use of tracers necessary for their navigation.

The Commission encourages not to use techniques for masking the identity of the entity using tracers, such as subdomain delegation.

The Commission also recommends that the names of the tracers used be explicit and, as far as possible, standardized regardless of the actor behind their emission.

Finally, the Commission encourages professionals to name the tracker allowing the choice of eu-consent users to be stored, by attaching to each purpose a Boolean true or false value memorizing the choices made. Article 7 - Publication in the Official Journal of the French Republic. This deliberation will be published in the Official Journal of the French Republic.

The president,

M. L. Denis