

Deliberation 2020-091 of September 17, 2020 Commission Nationale de l'Informatique et des Libertés Nature of the

deliberation: Opinion Legal status: In force Date of publication on Légifrance: Tuesday, October 06, 2020 NOR:

CNIL2026187X Deliberation n° 2020-091 of September 17, 2020 adopting lines guidelines relating to the application of article 82 of the law of January 6, 1978 as amended to read and write operations in a user's terminal (in particular to "cookies and other tracers") and repealing deliberation no. 2019- 093 of July 4, 2019 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;

Considering the decision of the Council of State n° 434684 of June 19, 2020;

Having regard to the guidelines on consent within the meaning of Regulation (EU) 2016/679 adopted on May 4, 2020 by the European Data Protection Board; After having heard Mr François PELLEGRINI, Commissioner, in his report, and Mr Benjamin TOUZANNE, Government Commissioner, in his observations, Adopts the following guidelines:

The National Commission for Computing and Liberties (hereinafter the Commission) is responsible for ensuring compliance with Article 82 of the law of January 6, 1978 referred to above (hereinafter the Computing and Liberties Act).

In this context, the main purpose of these guidelines is to recall and explain the law applicable to the operations of reading and/or writing information (hereafter tracers) in the electronic communications terminal equipment of the subscriber or user,

and in particular to the use of connection cookies (hereinafter cookies). The legal framework results in particular from the applicable provisions of the directive of July 12, 2002 referred to above (hereinafter the ePrivacy directive), transposed into national law in article 82 of the Data Protection Act, and from the definition of consent established in Article 4 of the aforementioned Regulation (EU) of April 27, 2016 (hereinafter GDPR), which the aforementioned guidelines of the European Data Protection Board (EDPS) are intended to clarify.

Article 82 of the Data Protection Act provides:

Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he has been informed beforehand, by the controller or his representative:

- 1° The purpose of any action seeking to access, by electronic transmission, information already stored in its electronic communications terminal equipment, or to enter information in this equipment;
- 2° The means at his disposal to oppose it.

This access or registration can only take place on condition that the subscriber or user has expressed, after having received this information, his consent which may result from appropriate parameters of his connection device or any other device placed under his control.

These provisions are not applicable if the access to information stored in the user's terminal equipment or the registration of information in the user's terminal equipment:

- 1° Either, has the exclusive purpose of allowing or facilitating communication by electronic means;
- 2° Or, is strictly necessary for the provision of an online communication service at the express request of the user.

These provisions thus impose the collection of consent before any action aimed at storing information or accessing information stored in the terminal equipment of a subscriber or user, apart from the applicable exceptions.

The Commission recalls that the consent provided for by these provisions, read in the light of Article 5 of the ePrivacy Directive and Article 94 of the GDPR, refers to the definition and the conditions provided for in Articles 4(11) and 7 of the GDPR.

The GDPR has clarified the conditions for obtaining consent and the need to demonstrate that it has been collected.

The entry into application of the GDPR thus led the Commission to repeal, by its deliberation n° 2019-093 of July 4, 2019, its 2013 recommendation relating to cookies and other trackers, to replace it with guidelines. This deliberation draws the consequences of the aforementioned decision of the Council of State of June 19, 2020 and updates these guidelines.

These guidelines are supplemented by non-prescriptive and non-exhaustive recommendations, presenting in particular examples and best practices of concrete methods of obtaining consent and implementing tracers not subject to the latter. Article 1 - On the scope of application of the guidelines.

The guidelines concern all operations aimed at accessing, by means of electronic transmission, information already stored in the terminal equipment of the subscriber or user of an electronic communications service or entering information in that -this.

Article 1 of Directive 2008/63/EC of 20 June 2008 referred to above defines terminal equipment as any equipment which is connected directly or indirectly to the interface of a public telecommunications network to transmit, process or receive information ; in both cases, direct or indirect, the connection can be established by wire, optical fiber or electromagnetic way; a connection is indirect if a device is interposed between the terminal equipment and the public network interface.

This definition encompasses many commonly used devices, such as a tablet, a smartphone (smartphone), a fixed or mobile computer, a video game console, a connected television, a connected vehicle, a voice assistant, as well as any other equipment terminal connected to a telecommunications network open to the public.

These guidelines apply to all terminal equipment covered by this definition, regardless of the operating systems or application software (such as web browsers) used.

They relate, in particular, to the use of HTTP cookies, by which these reading or writing actions are most often carried out, but also other technologies such as local shared objects sometimes called Flash cookies, local storage mis implemented within the HTML 5 standard, identification by calculation of the terminal fingerprint or fingerprinting, identifiers generated by operating systems (whether advertising or not: IDFA, IDFV, Android ID, etc.), hardware identifiers (MAC address, serial number or other identifier of a device), etc. For the purposes of these guidelines, the word tracer designates all the devices likely to be covered by article 82 of the law.

Finally, these guidelines concern the aforementioned operations of reading and writing any information stored or consulted in terminal equipment in the predefined sense, whether or not it concerns personal data within the meaning of the GDPR. The provisions of paragraph 3 of article 5 of the ePrivacy Directive and, consequently, of article 82 of the Data Protection Act, are indeed applicable to such operations regardless of whether the data concerned is personal. or not.

The Commission recalls that any processing relating to data produced or collected via a tracker, when these fall within the category of personal data - sometimes directly identifying (for example, an e-mail address) and often indirectly identifying (for

example, the unique identifier associated with a cookie, an IP address, an identifier of the terminal or of a component of the user's terminal, the result of the fingerprint calculation in the case of a fingerprinting technique, or even an identifier generated by software or an operating system) - must comply with the provisions of the GDPR and the relevant provisions of the Data Protection Act. These processing operations are not covered by these guidelines. Article 2 - On the procedures for obtaining consent.

Pursuant to the combined provisions of Articles 82 of the Data Protection Act and 4 of the GDPR, trackers requiring the collection of consent may only, subject to the exceptions provided for by these provisions, be used in writing or reading provided that the user has expressed his will for this purpose, in a free, specific, informed and unequivocal manner, by a declaration or by a clear positive act. Regarding the free nature of consent

In order to determine whether consent is freely given, the GDPR requires the utmost consideration to be given to whether, among other things, the performance of a contract, including the provision of a service, is conditional on consent. to the processing of personal data which is not necessary for the performance of this contract. According to Recital 42 of the GDPR, which clarifies the requirement of freedom of consent set out in its Article 4, consent should not be considered to have been freely given if the data subject does not have a real freedom of choice or is unable to refuse or withdraw consent without prejudice. Under these conditions, the Commission considers that the fact of making the provision of a service or access to a website subject to the acceptance of write or read operations on the user's terminal (so-called practice of cookie wall ) is likely to infringe, in certain cases, the freedom of consent.

In the event of the implementation of a cookie wall, and subject to the legality of this practice which must be assessed on a case-by-case basis, the information provided to the user should clearly indicate the consequences of his choices and in particular the impossibility of access content or service without consent.

Finally under the terms of recital 43 of the GDPR, consent is presumed not to have been given freely if separate consent cannot be given to different personal data processing operations although this is appropriate in the case at hand. In this regard, the Commission considers that the fact of simultaneously obtaining a single consent for several processing operations responding to distinct purposes (the coupling of purposes), without the possibility of accepting or refusing purpose by purpose, is also likely to affect, in certain cases, the freedom of choice of the user and therefore the validity of his consent. Regarding the specific nature of the consent

The Commission recalls that consent to read and write operations must be specific. As such, consent to these operations cannot be validly obtained via an overall acceptance of the general conditions of use. Regarding the informed nature of consent

The Commission recalls that the consent of individuals must be informed in accordance, on the one hand, with the provisions of Articles 4(11), 7, 13 of the GDPR and, on the other hand, with the provisions of Article 82 of the Data Protection Act. and Freedoms.

The Commission recalls that the information must be written in simple terms that can be understood by all and that it must allow users to be duly informed of the different purposes of the trackers used. It considers that the use of overly complex legal or technical terminology is likely to make this information incomprehensible to users.

The Commission points out that the information must be complete, visible and highlighted. A simple reference to the general conditions of use is not sufficient.

At a minimum, the provision of the following information to users, prior to obtaining their consent, is necessary to ensure the informed nature of the latter:

- the identity of the person(s) responsible for processing the read or write operations;
- the purpose of the data reading or writing operations;
- how to accept or refuse trackers;
- the consequences attached to a refusal or acceptance of tracers;
- the existence of the right to withdraw consent. The Commission recalls that in order for the consent to be informed, the user must be able to identify the controller(s) as well as all the joint controllers of the processing, before being put in able to express their choice. Thus, the exhaustive and up-to-date list of these entities must be made accessible in a simple way to users.

The Commission points out that, in accordance with Article 4(11) of the GDPR, consent must be manifested through a positive action by the person who has been informed beforehand of the consequences of his choice and who has the means to express it.

It therefore considers that continuing to browse a website, use a mobile application or scroll down the page of a website or a mobile application do not constitute clear positive actions that can be assimilated to valid consent. The Commission recalls that the Court of Justice of the European Union (CJEU) ruled in its Planet 49 decision of 1 October 2019 (CJEU, 1 Oct. 2019,

C-673/17) that the use of pre-ticked boxes cannot be considered as a clear positive act aimed at giving consent. In the absence of consent expressed by a clear positive act, the user must be considered as having refused access to his terminal or the registration of information in the latter.

Appropriate systems should be put in place to collect consent in a practical manner allowing users to benefit from easy-to-use solutions. On this point, the Commission refers to its recommendation no. 2020-092 of September 17, 2020. On proof of consent

Article 7.1 of the GDPR requires that the organizations operating trackers, responsible for the processing(s), be able to provide, at any time, proof of valid collection of the free, informed, specific and unequivocal consent of the user. refusal and withdrawal of consent

The Commission observes that if the consent must result in a positive action by the user, the latter's refusal can be deduced from his silence. The expression of the user's refusal must therefore not require any action on his part or must be able to result in an action presenting the same degree of simplicity as that allowing him to express his consent.

In addition, the Commission recalls that, in accordance with Article 7.3 of the GDPR, it must be as easy to withdraw consent as to give it. Users who have given their consent to the use of tracers must be able to withdraw it simply and at any time. Article 3 - On the qualification of the actors. The tracers concerned by the obligation to obtain consent do not imply systematically processing personal data. However, in a large number of cases, the read or write operations will concern personal data, the processing of which will be subject to the other provisions of the Data Protection Act and the GDPR.

If, in some cases, the use of tracers involves a single entity which is therefore fully responsible for the obligation to obtain consent (for example, a website editor who uses tracers to personalize the editorial content offered to the Internet user), in other cases, several actors contribute to the performance of the reading or writing operations covered by these guidelines (for example, a website publisher and an advertising agency depositing tracers during the consultation of the website). In the latter cases, these entities must determine their status with regard to the processing carried out. 3.1. Joint responsibility and obligations of those responsible for the processing(s)

The Commission recalls that the publisher of a site that deposits tracers must be considered as a data controller, including when it subcontracts to third parties the management of these tracers set up for its own account.

Third parties who use tracers on a service published by another organization must also be considered as data controllers, for

example by depositing tracers when visiting a publisher's site, when they act to their own account. In this case, the Council of State ruled, in its decision of June 6, 2018, that the obligations incumbent on the site editor include that of making sure with its partners, of on the one hand, that they do not issue, via the publisher's site, tracers that do not comply with the regulations applicable in France and, on the other hand, that of taking any useful steps with them to put an end to breaches.

Therefore, the organization that authorizes the use of trackers, including by third parties, from its site or mobile application, must ensure the effective presence of a mechanism to collect the consent of users.

In general, the Commission observes that the publishers of mobile sites or applications, because of the direct contact they have with the user, are often in the best position to bring to their attention the information on registered tracers and to collect their consent.

For transactions covered by Article 82, as the CJEU also ruled in a similar case (CJEU, 29 July 2019, case C-40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV), the publisher of the site or the mobile application and the third party depositing tracers are deemed to be joint controllers insofar as they jointly determine the purposes and means of the read and write operations on the terminal equipment users.

In the case of joint responsibility, in which the controllers jointly determine the purposes and means of the processing, the Commission recalls that, in accordance with the provisions of Article 26 of the GDPR, they must define their obligations in a transparent manner. for the purpose of ensuring compliance with the requirements of the GDPR, in particular with regard to the collection and demonstration, where applicable, of valid consent.

### 3.2. Subcontracting

The Commission recalls that an actor who stores and/or accesses information stored in a user's terminal equipment exclusively on behalf of a third party must be considered a subcontractor. It recalls, in this respect, that if a subcontracting relationship is established, the data controller and the subcontractor must draw up a contract or another legal act specifying the obligations of each party, in compliance with the provisions of the 28 GDPR.

The Commission also recalls that, in accordance with Article 28.3 of the GDPR, the processor must help the controller to comply with some of its obligations and in particular those relating to requests to exercise the rights of individuals.

Finally, the subcontractor must in particular inform the latter if one of its instructions constitutes a violation of the applicable texts on the protection of personal data.

Article 4 - On the parameters of the terminal.

Article 82 of the law specifies that consent may result from appropriate parameters of the person's connection device or any

other device placed under their control.

Nevertheless, on the date of adoption of these guidelines, the Commission considers, in the light of the knowledge at its disposal and without prejudice to possible technical developments, that the possibilities for configuring browsers and exploitation cannot, on their own, enable the user to express valid consent. Indeed, if web browsers offer many settings allowing users to express choices regarding the management of cookies and other tracers, these are generally expressed today under conditions that do not ensure a sufficient level prior information of persons, such as to comply with the principles set out in these guidelines.

In addition, browsers do not, to date, make it possible to distinguish tracers according to their purposes, even though this distinction may prove necessary to guarantee freedom of consent. Article 5 - On tracers exempt from consent.

As a reminder, the consent requirement does not apply to operations whose exclusive purpose is to allow or facilitate communication by electronic means or are strictly necessary for the provision of an online communication service at the express request of users. .

Tracers only fall outside the scope of the consent requirement if they are used exclusively for one or more purposes which may relate to the exceptions provided for in Article 82 of the Data Protection Act.

The Commission specifies, in this regard, that the use of the same tracker for several purposes, some of which do not fall within the scope of these exemptions, requires the prior consent of the persons concerned to be obtained, under the conditions recalled by the these guidelines. For example, in the case of a service offered via a platform requiring user authentication (logged universe), the service publisher may use a cookie to authenticate users without asking for their consent (because this cookie is strictly necessary for the provision of the online communication service). On the other hand, he will only be able to use this same cookie for advertising purposes if the latter have actually consented beforehand to this specific purpose.

Trackers exempt from obtaining consent

Based on the practices brought to its attention, the Commission considers that the following tracers can, in particular, be regarded as exempt:

- the tracers retaining the choice expressed by the users on the deposit of tracers;
- tracers intended for authentication with a service, including those intended to ensure the security of the authentication mechanism, for example by limiting robotic or unexpected access attempts;



- tracers intended to store the contents of a shopping cart on a merchant site or to invoice the user for the product(s) and/or services purchased;
- user interface personalization tracers (for example, for the choice of language or presentation of a service), when such personalization constitutes an intrinsic and expected element of the service;
- tracers enabling load balancing of equipment contributing to a communication service;
- tracers allowing paying sites to limit free access to a sample of content requested by users (predefined quantity and/or over a limited period);
- certain audience measurement trackers, subject to the reservations mentioned below. Specific case of audience measurement trackers

Managing a website or application almost always requires the use of traffic and/or performance statistics. These measures are in many cases essential for the proper functioning of the site or application and therefore for the provision of the service.

Consequently, the Commission considers that trackers whose purpose is limited to measuring the audience of the site or application, to meet various needs (measurement of performance, detection of browsing problems, optimization of technical performance or ergonomics, estimation of the power of the servers required, analysis of the content consulted, etc.) are strictly necessary for the operation and day-to-day administration of a website or an application and are therefore not subject, in application of article 82 of the Data Protection Act, to the legal obligation of prior collection of the consent of the Internet user.

In order to be limited to what is strictly necessary for the provision of the service, the Commission stresses that these tracers must have a purpose strictly limited to the sole measurement of the audience on the site or the application for the exclusive account of the editor. These tracers must in particular not allow the overall monitoring of the browsing of the person using different applications or browsing on different websites. Similarly, these tracers must only be used to produce anonymous statistical data, and the personal data collected cannot be cross-checked with other processing operations or transmitted to third parties, these different operations not being necessary for the operation of the service.

More generally, the Commission recalls that audience measurement processing is processing of personal data which is subject to all the relevant provisions of the GDPR. Article 6 - Repeal of deliberation no. 2019-093 of July 4 2019.

This deliberation repeals deliberation no. 2019-093 of July 4, 2019 adopting guidelines relating to the application of article 82 of the law of January 6, 1978 as amended to read and write operations in the terminal of a user.

This deliberation will be published in the Official Journal of the French Republic. The President,

M. L. Denis