

Deliberation 2019-093 of July 4, 2019 National Commission for Computing and Freedoms Legal status: Repealed Date of publication on Légifrance: Saturday July 20, 2019 NOR: CNIL1920776Z Deliberation No. 2019-093 of July 4, 2019 adopting guidelines relating to the application of article 82 of the law of January 6, 1978 amended to read or write operations in a user's terminal (in particular to 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 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;

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

Having regard to the guidelines on consent within the meaning of Regulation (EU) 2016/679 adopted on 10 April 2018 by the Article 29 Data Protection Working Party and endorsed by the European Data Protection Board (EDPB)) on May 25, 2018;

Having regard to the statement of 25 May 2018 from the European Data Protection Board on the revision of the privacy and electronic communications directive and its impact on the protection of privacy and the confidentiality of electronic communications;

Having regard to Opinion 5/2019 on the relationship between the Privacy and Electronic Communications Directive and the GDPR, in particular concerning the competence, tasks and powers of data protection authorities, adopted by the European Data Protection Board (EDPS) on 12 March 2019;

Having regard to deliberation no. 2013-378 of December 5, 2013 adopting a recommendation relating to cookies and other

tracers referred to in article 32-II of the law of January 6, 1978;

After having heard Mr. François PELLEGRINI, commissioner, in his report, and Mrs. Nacima BELKACEM, government commissioner, in her observations,

Adopts the following guidelines:

The National Commission for Computing and Freedoms (CNIL) is responsible for ensuring compliance with the provisions of Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms (hereinafter the Data Protection Act), as well as other texts relating to the protection of personal data.

The purpose of these guidelines is to recall the law applicable to read or write operations in a user's terminal, and in particular the use of cookies and other tracers. They result in particular from the provisions of Directive 2002/58/EC amended privacy and electronic communications (or ePrivacy) transposed into French law in Article 82 of the Data Protection Act, and from the definition of consent appearing in Article 4 of the General Data Protection Regulation (GDPR) as interpreted in the guidelines of the European Data Protection Board (EDPB).

In the event of a breach of these provisions, the Commission recalls that it may take all corrective measures and sanctions vis-à-vis the bodies subject to them, pursuant to Article 3 of the law, and this in particular independently of the provisions of Chapter VII of the GDPR on cooperation and consistency, insofar as Article 82 results from the transposition of a separate directive.

Article 82 of the law provides that:

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.

This article, which transposes article 5 (3) of the privacy and electronic communications directive, thus imposes 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 these guidelines only concern the implementation of the provisions of Article 82 of the Data Protection Act; any processing of personal data using data collected via read or write operations must also comply with all applicable legal provisions.

The consent provided for by these provisions must comply with the definition and the conditions provided for in Articles 4 (11) and 7 of the GDPR.

The GDPR has reinforced the requirements for people's consent, by providing clarifications on the conditions for obtaining it and on the need to demonstrate that it has been collected.

The strengthening of the rights of individuals leads the Commission to repeal its deliberation n° 2013-378 of December 5, 2013 adopting a recommendation relating to cookies and other tracers covered by article 32-II of the law of January 6, 1978 (hereinafter the cookie and other tracers recommendation) to replace it with these guidelines. These guidelines will be supplemented later by sectoral recommendations aimed in particular at specifying the practical methods of obtaining consent. Article 1

On the scope of the guidelines.

These guidelines apply to all operations aimed at accessing, by electronic transmission, information already stored in the subscriber's or user's terminal or at recording information in this equipment.

The Commission notes that Article 1 of Directive 2008/63/EC 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 multifunctional mobile (smartphone), a fixed or mobile computer, a video game console, a connected television, a connected vehicle, a voice assistant, as well as any other object connected to a telecommunications network open to the public.

These guidelines apply regardless of the operating systems, application software (such as browsers) or terminals used.

The guidelines relate to the use of HTTP cookies, by which these actions are most often carried out, but are also intended to

apply to the use of other techniques: local shared objects (sometimes called Flash cookies, local storage (local storage) implemented within HTML 5, identifications by calculating the fingerprint of the terminal, identifiers generated by operating systems (whether advertising or not: IDFA, IDFV , Android ID, etc.), hardware identifiers (MAC address, serial number or any other identifier of a device), etc. For the purposes of these guidelines, the word tracer will designate all the devices covered by article 82 of the law.

Whether or not the information (stored and/or accessed) is personal data within the meaning of the GDPR is not a prerequisite for the application of Article 5(3) of Directive 2002/58/ THIS. Consequently, the aforementioned Article 82 applies regardless of whether the data concerned is of a personal nature or not.

Finally, the Commission draws the attention of the organizations concerned to the fact that any processing relating to a tracker, when it falls within the category of personal data - sometimes directly identifying (for example, an e-mail address) and often indirectly identifying (for example, the unique identifier of 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 technical fingerprinting, or an identifier generated by software or an operating system) - requires compliance with the provisions of the GDPR. Article 2

On the methods of obtaining consent.

In application of the Data Protection Act, the GDPR and the EDPS guidelines on consent, tracers requiring the collection of consent cannot be used in writing or reading until the user has previously expressed this end his will, in a free, specific, informed and unequivocal manner by a declaration or by a clear positive act.

With regard to the free nature of consent

The Commission considers that consent can only be valid if the person concerned is able to validly exercise his choice and does not suffer major disadvantages in the event of the absence or withdrawal of consent.

In this respect, the Commission recalls that the EDPS, in his statement on the revision of the ePrivacy Directive and its impact on the protection of private life and the confidentiality of electronic communications, considered that the practice of blocking access to a website or mobile application that does not consent to being tracked (cookie walls) is not GDPR compliant. The EDPS considers that, in such a case, users are not in a position to refuse the use of tracers without suffering negative consequences (in this case the impossibility of accessing the site consulted).

With regard to the specific nature of consent

The Commission recalls that the data subject must be able to give their consent independently and specifically for each distinct purpose. The fact of offering the person in addition the possibility of consenting in a global way is acceptable, provided that this is in addition to, without replacing it, the possibility of consenting specifically for each purpose.

As such, the overall acceptance of general conditions of use cannot be a valid method of obtaining consent, insofar as it cannot be given separately for each purpose.

With regard to the informed nature of consent

The Commission recalls that the information must be written in simple and understandable terms for all, and that it must allow users to be fully informed of the different purposes of the trackers used. It considers that the use of too complex legal or technical terminology does not meet the requirement of prior information.

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

The information that must be brought to the attention of users, prior to obtaining consent, pursuant to Article 82, is at least:

- the identity of the controller(s);
- the purpose of the data reading or writing operations;
- the existence of the right to withdraw consent.

When processing of personal data follows the read or write operation and this is based on consent, the prior information given to users must then be completed in order to meet the requirements of the EDPS guidelines on the consent.

The Commission recalls that in order for consent to be informed, the user must be able to identify all the entities using trackers before being able to consent. Thus, the exhaustive and regularly updated list of these entities must be made available to the user directly when obtaining his consent.

With regard to the unequivocal nature of consent

The Commission emphasizes that consent must be manifested through positive action by the person who has been informed beforehand of the consequences of his choice and who has the means to exercise it. Continuing to browse a website, use a mobile application or scroll down the page of a website or mobile application do not constitute clear positive actions that amount to valid consent.

It also considers that the use of pre-ticked boxes, as well as the general acceptance of general conditions of use, cannot be

considered as a clear positive act aimed at giving its consent.

Appropriate systems must therefore be put in place to collect consent in practical ways that allow users to benefit from user-friendly and ergonomic solutions.

On proof of consent

Article 7 of the GDPR requires that consent be demonstrable, which means that organizations operating tracers must implement mechanisms allowing them to demonstrate, at any time, that they have validly obtained the consent of users. In the situation where these organizations do not themselves obtain the consent of individuals, the Commission points out that such an obligation cannot be fulfilled simply by the presence of a contractual clause committing one of the organizations to obtain valid consent for the other party's account.

On the withdrawal of consent

The Commission points out that it must be as easy to refuse or withdraw consent as to give it. This means in particular that people who have given their consent to the use of tracers must be able to withdraw it at any time. User-friendly solutions must therefore be implemented so that people can withdraw their consent as easily as they were able to give it. Article 3

On the roles and responsibilities of the actors.

The technologies concerned by the obligation to obtain consent do not systematically involve the processing of personal data. However, in a large number of cases, the read or write operations will concern personal data and will be an integral part of the processing of personal data subject to the other provisions of the law and the GDPR, which implies the need to qualify the parties involved.

If, in a certain number of cases, the use of tracers involves a single entity which is therefore fully responsible for the obligation to obtain consent (for example, a website publisher who uses tracers to carry out even the usage statistics of its service), in other cases, several actors contribute to the performance of the read or write operations covered by these guidelines (for example a website publisher and an advertising network depositing cookies when visiting the website). In the latter case, these entities may be considered as sole controllers, joint controllers or as processors.

The Commission notes that, in other cases, third parties using trackers will be fully and independently responsible for the trackers they use, which means that they will have to independently assume the obligation to obtain the consent of users. .

In the case of joint responsibility, in which the controllers jointly determine the purposes and means of the processing, the

Commission recalls that under the terms of Article 26 of the GDPR, they will have to define in a transparent manner their respective obligations for the purposes of ensure compliance with the requirements of the GDPR, in particular with regard to the collection and demonstration, where applicable, of valid consent.

Finally, a subcontractor is qualified as an actor who enters information and/or accesses information stored in the terminal equipment of a subscriber or user, exclusively on behalf of a data controller and without reuse. for its own account of the data collected via the tracker. The Commission recalls that if a subcontracting relationship is established, the controller and the processor must draw up a contract or another legal act specifying the obligations of each party, in compliance with the provisions of Article 28 of the GDPR. Article 4

On terminal settings.

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.

The Commission considers that these browser settings cannot, in the state of the art, allow the user to express valid consent. First of all, if web browsers offer many settings allowing users to express choices in terms of cookies, it is clear that these are expressed under conditions that do not ensure a sufficient level of prior information to people.

Next, whatever the existing mechanisms, browsers do not allow cookies to be distinguished according to their purposes, which means that the user is also not able to consent specifically for each purpose.

Finally, the browser settings do not currently allow you to express a choice on technologies other than cookies (such as fingerprinting for example) for the purpose of monitoring navigation.

However, browsers may evolve to incorporate mechanisms to collect GDPR-compliant consent. The Commission considers that such a development would be likely to guarantee, on the one hand, that Internet users have effective and simple tools allowing them to consent in a simple way and, on the other hand, that publishers who do not have resources or powers to put in place mechanisms for obtaining consent can be based on such mechanisms. Article 5

On the specific case of audience measurement tracers.

A publisher may need to measure the audience of his website or application, or to test different versions in order to optimize his editorial choices according to their respective performance. Tracers are frequently used for this purpose and these devices may, in certain cases, be regarded as necessary for the provision of the service explicitly requested by the user, without being

particularly intrusive for them, and thus be exempted from the collection of consent. For example, traffic statistics and tests aimed at measuring the relative performance of different versions of the same website (commonly called A/B tests) allow publishers to detect navigation problems in their site or application or yet to organize the contents.

Therefore, the Commission considers that can benefit from this exemption to the collection of consent, processing that meets the following conditions:

- they must be implemented by the publisher of the site or by its subcontractor;
- the person must be informed prior to their implementation;
- it must have the ability to oppose it via an easily usable opposition mechanism on all terminals, operating systems, applications and web browsers. No read or write operation should take place on the terminal from which the person objected;
- the purpose of the device must be limited to (i) the audience measurement of the content viewed in order to allow the evaluation of the published content and the ergonomics of the site or application, (ii) the segmentation of the audience of the website in cohorts in order to assess the effectiveness of editorial choices, without this leading to targeting a single person and (iii) the dynamic modification of a site globally. The personal data collected must not be cross-checked with other processing (customer files or statistics of visits to other sites, for example) or passed on to third parties. The use of tracers must also be strictly limited to the production of anonymous statistics. Its scope must be limited to a single site or mobile application publisher and must not allow the tracking of the navigation of the person using different applications or browsing different websites;
- the use of the IP address to geolocate the Internet user must not provide more precise information than the city. The IP address collected must also be deleted or anonymized once the geolocation has been carried out;
- the tracers used by these treatments must not have a lifespan exceeding thirteen months and this period must not be automatically extended during new visits. The information collected through tracers must be kept for a maximum of twenty-five months. Article 6

On read or write operations not subject to prior consent.

Article 82 provides that the prior consent requirement does not apply if the access to information stored in the user's terminal equipment or the recording of information in the user's terminal equipment:

- has the exclusive purpose of allowing or facilitating communication by electronic means; Where

- is strictly necessary for the provision of an online communication service at the express request of the user.

Nor does the law require offering the possibility of opposing the use of tracers allowing or facilitating communication by electronic means, or even strictly necessary for the provision of an on-demand online communication service. expressed by the user.

However, in order to ensure full and complete transparency on these operations, users must be informed of their existence and their purpose by including, for example, a mention in the confidentiality policy of the organizations using them. Article 7

Repeal of recommendation no. 2013-378 of December 5, 2013.

This deliberation repeals deliberation no. 2013-378 of December 5, 2013 adopting a recommendation relating to cookies and other tracers covered by article 32-II of the law of January 6, 1978.

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

The president,

M. L. Denis