# Questions and answers on the amending guidelines and the CNIL "cookies and other tracers" recommendation

March 18, 2021

The CNIL answers questions about its guidelines and its recommendation on the use of cookies and other tracers.

General questions

1. What is the relationship between the guidelines and the recommendation?

The CNIL guidelines on cookies and other tracers aim to recall the law applicable to reading or writing operations in the terminal (smartphone, computer, tablet, etc.) of an Internet user.

The aim of the recommendation is to guide the professionals concerned in their compliance process, without however being prescriptive. It offers examples of practical procedures for obtaining consent in accordance with applicable rules but also to meet the requirements of Article 82 of the Data Protection Act.

2. Why have the July 4, 2019 guidelines been adjusted?

The guidelines of July 4, 2019 were notably adjusted to take into account the decision of the Council of State of June 19, 2020.

3. What are the main new features compared to the 2013 recommendation?

The entry into force of the General Data Protection Regulation (GDPR) on May 25, 2018, clarified the conditions for obtaining consent and the need to demonstrate that it has been collected. The main new features compared to the 2013 recommendation are as follows:

- Merely continuing to browse a site can no longer be considered a valid expression of the user's consent to the use of tracers. The recommendation gives several examples of practices allowing unambiguous collection of consent.
- The recommendation proposes different practical methods of collecting consent as well as refusal of the user.
- It recommends several ways for actors to provide the identity of those responsible for the processing (s) to which the person gives their consent.
- It proposes practical methods by which those responsible for the processing (s) who deposit tracers can provide proof of consent.

4. What will be the repressive policy of the CNIL? What timetable?

Sites using cookies and other tracers will be subject to compliance actions during 2021. The CNIL action plan has two phases:

The first phase, which began in October 2020 when the guidelines and the recommendation were published, focused the actions of the CNIL on compliance with the principles previously set out in the 2013 recommendation. Corrective measures, including sanctions, may be adopted in the event of non-compliance with obligations, the scope of which has been specified since 2013 and which continue in the new guidelines.

In the second phase, from April 2021, monitoring missions on the application of the entire legal framework in force, informed by the new guidelines, will be carried out.

In accordance with the case law of the Council of State, the CNIL is at any time in a position to prosecute breaches that seriously infringe the right to data protection and respect for privacy (CE, 16 Oct. 2019, no. ° 433069, Rec.).

5. Where is the draft European “ePrivacy” regulation?

Article 82 of the Data Protection Act is the national transposition of the provisions of Article 5 (3) of Directive 2002/58 / EC of July 12, 2002 known as "ePrivacy", amended in 2009.

In 2017, a proposal for a regulation from the European Commission was published to revise this directive. This revision was announced in 2016 with a view to harmonizing with the GDPR and is part of the work carried out on the digital single market strategy announced by the European Commission in May 2015.

While Parliament adopted its position on the text at the end of 2017, the twenty-seven representatives of the Member States finally agreed, on February 10, 2021, on a negotiating mandate for the revision of these rules. The agreement reached allows the Council of the European Union to start negotiations with the European Parliament on the final text.

6. Are public bodies concerned?

Yes.

The guidelines and the recommendation concern both private and public organizations as soon as they are subject to the obligations of the Data Protection Act and carry out the reading and / or writing operations referred to in the article. 82 of the law.

7. Do the provisions of article 82 of the Data Protection Act apply to the deposit of tracers within an intranet?

No.

The provisions of article 82 of the Data Protection Act, read in the light of the “ePrivacy” directive, do not apply to an intranet when it is not an open telecommunications network. to the public.

However, any processing of personal data implemented as part of the management of an intranet must comply with all the provisions of the GDPR (information to individuals, legal basis, etc.).

8. Can the CNIL intervene with regard to tracers who do not collect personal data?

The provisions of Article 82 of the Data Protection Act apply regardless of whether the information collected through these tracers is personal data or not.

The CNIL is responsible for ensuring the compliance of any data processing falling within the scope of the law, whether or not it concerns personal data. However, the provisions relating to tracers are found in this law.

**Audience measurement tracers**

9. Are tracers used for audience measurement exempt from consent?

Yes, under certain conditions.

It is not necessary to obtain the user's consent, if these tracers are strictly necessary for the provision of an online communication service expressly requested by the user, in accordance with article 82 of the Data Protection Act and Freedoms. The CNIL considers that audience measurement can, to a certain extent, be regarded as strictly necessary for the operation of the site. In order to limit itself to this, the CNIL reminds that tracers must:

- be strictly limited to the sole measurement of audience on the site for the exclusive account of the publisher;
- be used only to produce anonymous statistical data;
- not allow the overall tracking of the navigation of the person using different applications or browsing different websites;
- not to allow the data to be cross-checked with other processing or for the data to be transmitted to third parties.
- These guarantees are recalled in article 5 of the "cookies and other tracers" guidelines. Any data controller must be able to demonstrate their compliance when using an audience measurement solution without the user's consent being obtained.

In addition, audience measurement processing remains, by its nature, processing of personal data which is subject to all the obligations of the GDPR.

Learn more about audience measurement tools.

10. Can audience measurement solutions that allow anonymization of the data collected benefit from an exemption from the consent provided for in Article 82 of the Data Protection Act?

Only audience measurement tracers strictly necessary for the provision of an online communication service expressly requested by the user are exempt from consent.

In order to be limited to what is strictly necessary for the provision of the service, these tracers must in fact only be used to produce anonymous statistical data. However, other guarantees must also be implemented, as recalled in question 9.

Note: anonymity should be understood within the meaning given by the regulations on the protection of personal data. Pseudonymization (simple deletion of name or other identifying data) is not anonymization within the meaning of the regulations. European data protection authorities define three criteria that help ensure that a dataset is truly anonymous.

Learn more about data anonymization.

11. Does the CNIL plan to list, on its website, audience measurement solutions that can take advantage of the consent exemption?

Yes.

Aware of the need to help stakeholders identify audience measurement solutions whose settings allow them to take advantage of the exemption from the collection of consent, the CNIL is implementing a system enabling solution providers to check with of its services, the possibility of availing itself of such an exemption.

The objective is to identify whether the available configuration elements can allow the suppliers concerned to offer their customers an audience measurement offer exempt from the need to collect consent.

She will publish, on her website, a list of solutions selected.

Exempt tracers (excluding audience measurement)

12. Are the trackers used for billing affiliate transactions exempt from consent?

No.

The tracers used for invoicing affiliation transactions do not fall under the exemptions of Article 82 of the Data Protection Act, which must be interpreted strictly. Indeed, these operations are not intended exclusively to allow or facilitate electronic communication and are not strictly necessary for the provision of an online communication service expressly requested by the user.

13. Is the use of trackers for anti-fraud purposes (in the context of operating an e-commerce site or online banking, for example) exempt from consent?

The CNIL has listed, in article 5 of the "cookies and other tracers" guidelines, the main tracers which, in the state of the practices brought to its attention, are exempt from consent.

If the tracers used for the purposes of combating fraud, in general, do not fall within the exemptions provided for by article 82 of the Data Protection Act, the CNIL considers that this may be the case in certain specific cases. . This is particularly the case with those intended to ensure the security of a user authentication mechanism (for example, by limiting robotic or unexpected access attempts), which may be considered necessary for the communication service in line requested by the user.

14. Should the use of tracers which do not require the user's consent (so-called "functional" tracers for example) be the subject of information?

While article 82 of the Data Protection Act does not require users to be informed about the use of such tracers, the CNIL recommends that they be informed of their existence in order to ensure full transparency on these operations.

It should be noted that this information can be delivered within the policy relating to cookies.

In addition, and regardless of the obligations of Article 82, people must be informed in accordance with the GDPR of all processing of personal data implemented by publishers of mobile sites or applications.

Collecting consent

15. Can the continuation of navigation constitute acceptance of the tracers?

No.

If, under the regime prior to the GDPR, the CNIL considered that continuing to browse allowed Internet users, under certain conditions, to express their consent to the deposit of tracers, it must now be interpreted as a refusal to consent. In this case, no tracker requiring the user's consent can be placed or read on his terminal.

Indeed, the user's consent must materialize in a clear positive act such as, for example, clicking on an "accept all" button. The absence of a clear manifestation of willingness to accept the placement of a cookie should be understood as a refusal.

This notable development stems from the entry into force of the GDPR, which now requires unambiguous consent from the Internet user.

16. Can a website refer to browser settings to collect user consent?

No.

In the state of the art, and subject to possible future developments, the possibilities of configuring browsers and operating systems cannot, by themselves, allow the user to express valid consent.

17.?

Yes, under certain conditions.

In its recommendation, the CNIL recalls that in principle, it is necessary to keep the choices expressed by the user, whether it is his consent or his refusal. Thus, while browsing the website, they will not have to reformulate their choice from page to page.

In general, it is therefore recommended to save the choice expressed by the Internet user so as not to request them again for a certain period of time.

The retention period of the choices should be assessed on a case-by-case basis (with regard to the nature of the website or application concerned and the specificities of its audience). Generally, it is good practice to keep the choices for a period of 6 months.

18. Does the fact of offering sharing features on social networks imply the collection of the user's consent?

In general, social network buttons allow these third parties to place or read trackers on the user's terminal for purposes other than interaction with the social network in question (advertising purposes, etc.).

In such a case, the consent of the Internet user is required, in accordance with art.

18. Does the fact of offering sharing features on social networks imply the collection of the user's consent?

In general, social network buttons allow these third parties to place or read trackers on the user's terminal for purposes other than interaction with the social network in question (advertising purposes, etc.).

In such a case, the consent of the Internet user is required, in accordance with article 82 of the Data Protection Act.

19. Can the user information on the trackers be located under the "refuse all" and "accept all" buttons, on the first level of information?

In order for the user's consent to be informed, all of the information referred to in Article 2 of the "cookies and other tracers" guidelines must be available at the time of collecting their choice. It is recommended, on the first level of information, to clearly indicate the purposes of cookies, to allow the user to access the list of those responsible for the processing (s) via, for example, a hypertext link or a button. accessible from the first level of information, to inform them about the possibility of withdrawing consent at any time and, when relevant, of the consequences arising from a refusal of cookies.

The CNIL recalls that the information must be complete, visible and highlighted. In order not to mislead users, it also invites data controllers to ensure that the interfaces for collecting choices do not incorporate potentially misleading design practices aimed at or likely to bias the consent of users. Internet users.

20. Should a website allow the user to give consent only to certain companies?

While the regulations do not require the user to make an individual choice for each data controller, such a possibility may allow him to give more control over his data.

In any case, the CNIL recalls that it is necessary to provide the person concerned with information including the exhaustive list of data controllers concerned by the filing and reading of tracers subject to consent. In practice, the CNIL recommends including information on the identity of data controllers at the first level of information via a hypertext link or a button accessible from this level, referring to this list or to the second level of information.

21. What information must be provided within the list of third parties who place or read tracers on the user's terminal?

In order for their consent to be informed, users must be able to ascertain the identity of all those responsible for the processing (s), including joint controllers. The CNIL recommends including a link to their privacy policy in addition to the precise identity and purposes pursued by each of them.

Finally, the recommendation (section 2.3) proposes practical methods of implementing these principles.

22. With what degree of detail the purposes pursued must be presented to the user?

All the purposes of the trackers must be presented to users before they are offered the possibility of consenting or refusing. The CNIL recalls that it is essential to ensure that these are formulated in an intelligible manner, in an appropriate and sufficiently clear language.

In this regard, the CNIL recommends that each purpose be highlighted in a short and highlighted title, accompanied by a brief description. It provides, in paragraph 13 of its recommendation "cookies and other tracers", examples of purposes identified in the context of the consultation as well as the public consultation carried out on the recommendation.

The CNIL emphasizes that it is not necessary to indicate, on the first level of information, all the technical operations or all the tracers contributing to the same precisely determined purpose. A more detailed description of the purposes can be made available to the user (under a drop-down button, via a hypertext link made available at the first level of information, etc.).

For example, the use of tracers for the purposes of "advertising capping", the fight against "click fraud", billing for the display service or even to measure targets with a greater appetite for advertising. advertising to better understand the audience, generally used for displaying personalized advertising, may be mentioned in this additional information when these operations contribute to this more general purpose.

23. Can the Internet user withdraw his consent to the deposit of tracers after having given it?

Yes.

negate his decision at any time. The general principle is that it should be as easy to withdraw consent as it is to give it.

In practice, it is recommended that the solutions allowing the user to manage and withdraw his consent be easily accessible throughout his navigation, for example:

- by providing a link accessible at any time from the service concerned which will bear a descriptive name such as "manage my cookies";

- or through a configuration module accessible on all pages of the site by means of a "cookie" icon (located for example at the bottom left of the screen).

- In general, to ensure that the withdrawal of consent can be done simply and at any time, it is recommended that the mechanism for managing and withdrawing consent be placed in an area that attracts the user's attention or in areas where he expects to find it, and that the visuals used are as explicit as possible.

24. Are examples of interfaces for obtaining consent in a compliant manner offered by the CNIL?

The CNIL offers examples of interfaces in order to concretely illustrate the proposals made in the recommendation. It also provides actors with an example of a banner to offer a clear and simple choice to the user.

25. Is the delegation of subdomains (or “CNAME cloaking”) to deposit cookies legal? Does it prevent the collection of consent?

In principle, the delegation of subdomains is not contrary to the regulations on the protection of personal data. However, it is necessary to comply with the information requirements (in particular with regard to the identity of the person responsible for the processing (s)) and the collection of consent (when applicable).

However, it should be noted that the improper implementation of such a process can lead to security breaches. In concrete terms, third parties may be able to read authentication tokens stored in cookies, which may be particularly sensitive in the case of certain online services (insurance, banking, etc.).

26. What does the CNIL say about cookie walls?

The practice of the "cookie wall" is to block access to a website or a mobile application for the user who does not give his consent.

The implementation of a "cookie wall" is likely, in certain cases and under certain conditions, to infringe the freedom of consent. Thus, the lawfulness of using a "cookie wall" must be assessed on a case-by-case basis.

In any event, if a "cookie wall" is set up, and subject to its lawfulness, the information provided to the user must clearly indicate the consequences of his choices and, for example, the 'inability to access content or service without consent.

27. Some choice collection interfaces mention legitimate interest as a legal basis for the processing of personal data from tracers. What does the CNIL think?

The CNIL recalls that it is necessary to distinguish:

- on the one hand, the deposit and reading of the tracers on the user's terminal: the application of the provisions of article 82 of the Data Protection Act to these processing operations requires the prior collection of the consent of the user, subject to applicable exceptions;

- on the other hand, processing based on information from these tracers, which must be based on one of the legal bases provided for in Article 6 of the GDPR. The European Data Protection Board considers that consent will, in general, be the most appropriate legal basis, particularly in the context of processing carried out for advertising purposes. However, it is up to each controller to determine, on a case-by-case basis, the most suitable legal basis for their data processing.

Even when the data controller considers that the use he will make of the data collected by the tracers is based on the legitimate interest, such processing will only be possible if the tracers are accepted for the specified purposes since, in case of refusal, the data cannot be collected.

28. Can a website offer contextual advertising if the user refuses the deposit of trackers?

Contextual advertising covers all the advertising techniques which consist in targeting an audience according to the context in which the individual exposed to the message finds himself. Thus, unlike personalized advertising, it does not rely on tracking user navigation.

While the simple display of contextual advertising does not, in principle, require the use of tracers, the CNIL notes that, in many cases, tracers requiring the consent of the ut users are used to measure advertising performance (for example "capping" cookies, advertising audience measurement or the fight against click fraud).

29. Should a website obligatorily allow the Internet user to refuse the deposit of tracers?

Yes.

Any website that uses tracers must offer the Internet user a way to refuse them when they are not strictly necessary for the operation of the site or for an online communication service requested by the Internet user.

30. Is the integration of a "refuse all" button at the same level and in the same forms as the "accept all" button mandatory?

Yes, or failing that, another solution making it possible to refuse as easily as to accept must be presented to the Internet user.

If the modalities for proposing the refusal are free, it must however be as easy to accept as to refuse the tracers. Thus, the refusal must be able to either be deduced from the silence of the Internet user, or be manifested by an action as simple as that allowing to accept.

For example, the CNIL considers that the integration, at the stage of the first level of information for the Internet user, of a button "refuse all", at the same level and with the same aspect as the button "accept all", constitutes a clear and simple way to allow the user to express his choices.

In any case, the Internet user must be clearly informed of the means at his disposal to refuse the tracers, in particular when these means are less explicit than a button "refuse all" (user silence, continuation of his navigation without click on any option offered by the cookie management banner, etc.).

31. Can the user's refusal be collected only on the second level of information (for example by clicking on a "configure your choices" button) if the user is explicitly informed?

No.

While the modalities for proposing the refusal are free, the CNIL strongly recommends that the mechanism for expressing a refusal be accessible on the same screen and with the same ease as the mechanism for expressing consent.

Indeed, the CNIL considers that the fact of being able to consent in a single click when several actions are necessary to "configure" a refusal (a click on "configure your choices" and a click on "refuse all" for example) tends to bias the choice of the user, who wants to be able to view the site or use the application as quickly as possible.

32. Can a website use a different design (color, size, shape) for the “accept all” and “reject all” buttons?

The design of the interfaces for collecting the choices is left to the discretion of the publisher, provided that it does not seek to deceive the user or to make it more complex to refuse the tracers than to consent to them.

Thus, in order not to mislead users, the CNIL recommends that data controllers ensure that interfaces do not incorporate potentially misleading design practices that lead users to believe that their consent is mandatory or that visually put more worth one choice over another.