SOULIER BUNCH

Published on 11 March 2021

Soulier Bunch, Cabinet d'avocats d'affaires basé à Paris et Lyon

Read this post online

Cookies and trackers: Are your websites and mobile apps compliant?

When visiting a website or using mobile apps, users must be informed and give their consent before cookies or other trackers are deposited or read, unless these trackers benefit from one of the exemptions provided for by law.

Following the publication of its guidelines and recommendation on October 1, 2020, the *Commission Nationale de l'Informatique et des Libertés* (French Data Protection Authority, hereinafter the "CNIL") has given until March 31, 2021 to bring websites and mobile apps into compliance with the new rules.

What is a cookie or a tracker?

The terms "cookie" or "tracker" cover for example:

- HTTP cookies,
- "flash" cookies,
- the result of the calculation of a unique fingerprint of the terminal in the case of "fingerprinting" (calculation of a unique identifier of the terminal based on elements of its configuration for tracking purposes),
- invisible pixels or "web bugs",
- any other identifier generated by software or an operating system (serial number, MAC address, Unique terminal identifier (IDFV), or any set of data used to calculate a unique fingerprint of the terminal (for

example via a “fingerprinting” method).

They can be placed and/or read, for example when consulting a website, a mobile app., or installing or using software, regardless of the type of terminal used: computer, smartphone, digital tablet or video game console connected to the Internet.

What does the law say?

Article 5(3) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, commonly referred to as the “ePrivacy Directive”, laid down the following principle:

- the user must give his/her consent prior to the storage of information in his/her terminal equipment or the access to information already stored in such equipment;
- unless such actions are strictly necessary in order to provide an online communication service explicitly requested by the user or exclusively intended to carry out or facilitate the transmission of a communication over an electronic communications network.

Article 82 of the French Data Protection Act, which transposed said provisions into domestic law, stipulates as follows:

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

1° The purpose of any action to access, by electronic transmission, information already stored in his/her electronic communications terminal equipment, or to record information in such equipment;

2° The means at his/her disposal to oppose it.

Such access or recording may only take place if the subscriber or user has expressed, after having received this information, his/her consent, which may result from appropriate parameters of his/her connection device or any other device under his control.

These provisions shall not apply if access to information stored in the user’s terminal equipment or registration of information in the user’s terminal equipment:

1° either has the exclusive purpose of allowing or facilitating communication by electronic means, or

2° is strictly necessary for the provision of an online communication service at the express request of the user.”

The CNIL has recalled that the consent provided for by these provisions refers to the definition and conditions set out in Articles 4(11) and 7 of the GDPR. It must therefore be free given, for a specific purpose, informed, unambiguous and the user must be able to withdraw it at any time, as easily as he/she gave it.

In order to recall and clarify the law applicable to the deposit and reading of trackers in the user's terminal, the CNIL adopted guidelines[1] on September 17, 2020 and a recommendation[2]. The CNIL allowed six months to comply, i.e., compliance must be achieved by March 31, 2021 at the latest.

Which cookies require prior consent?

All cookies that do not have the exclusive purpose of allowing or facilitating communication by electronic means or that are not strictly necessary for the provision of an online communication service at the express request of the Internet user require the prior consent of such user.

Cookies that require prior information and the collections of the user's prior consent include:

- cookies used for targeted advertising purposes;
- social media cookies, in particular those generated by share buttons.

Cookies that do not require the prior consent of the user include in particular:

- trackers keeping the choice expressed by users on the use of trackers;
- trackers intended for authentication to a service, including those intended to ensure the security of the authentication mechanism, for example by limiting robotized or unexpected access;
- trackers designed to keep track of the content of a shopping cart on a merchant site or to bill the user with the product(s) or service(s);
- interface customization trackers (e.g., for the choice of language or presentation of a service), where such customization is an intrinsic and expected element of the service;
- trackers allowing load balancing of equipment contributing to a communication service;
- trackers allowing paying sites to limit free access to a part of their content requested by users (predefined quantity and/or over a limited period of time);
- trackers enabling audience measurement insofar as they meet certain conditions.

How to obtain a valid consent?

Consent must be expressed by an affirmative action of the person who must be informed beforehand, in particular, of the consequences of his/her choice and be given the means to accept, refuse and withdraw his/her consent.

Appropriate systems must therefore be put in place to collect consent according to practical terms and conditions that allow Internet users to benefit from solutions that are easy to use.

In its recommendation, the CNIL provided examples of how such solutions could be implemented.

The key takeaways are as follows:

- In other words, as long as the person has not given his/her consent, cookies may not be deposited or read on his/her terminal;

- The validity of the consent is therefore linked in particular to the quality of the information received. In concrete terms, it must be visible, highlighted, and written in simple terms that can be understood by any user. It is possible to have two levels of information: for example, a first level may briefly describe each purpose of the processing, and then a second level that provides more details on these purposes and on the list of data controller(s);
- The user must be able to accept or refuse the deposit and/or reading of cookies with the same degree of simplicity;
- . In concrete terms, solutions enabling users to withdraw their consent must be made available to the user and accessible at all times.

How to prove consent?

Beware, operators that set such cookies and trackers must be able to prove that they have obtained consent!

The CNIL has provided a few examples of how to do so:

- putting the code used by the organization collecting the consent, for the different versions of its site or mobile app, in escrow with a third party or even simply publishing on a public platform of a time-stamped hash of this code to be able to prove its authenticity *a posteriori*;
- a screenshot of the visual rendering displayed on a mobile or desktop device can be kept, on a time-stamped basis, for each version of the site or app.; or
- regular audits of the consent collection mechanisms implemented by the sites or apps from which consent is collected may be implemented by third parties empowered for this purpose;
- time-stamped retention, by third parties publishing these solutions, of information relating to the tools implemented and their successive configurations (such as consent collection solutions, also known as the CMP, i.e., “Consent Management Platform”).

What is the risk?

Article 20 of the French Data Protection Act lists the various measures/penalties that the CNIL can take/impose in the event of an infringement.

Fines may not exceed 10 million euros or 2% of the total annual worldwide turnover achieved during the preceding financial year, whichever is higher.

Under the assumptions set forth in Articles 83 §5 and §6 of the GDPR (which include, in particular, the rules governing consent and the rights of the data subjects), these caps are increased to 20 million euros and 4% of said turnover, respectively.

In determining the amount of the fine, the CNIL takes into account the criteria specified in said Article 83.

[1] Deliberation No. 2020-091 of September 17, 2020 adopting guidelines relating to the application of Article 82 of the Law of January 6, 1978 (i.e., French Data Protection Act), as amended, to reading or writing operations in a user's terminal (in particular "cookies and other trackers") and repealing Deliberation No. 2019-093 of July 4, 2019. See article entitled The French Data Protection Authority releases new guidelines for cookies published on our Blog in September 2019. Such guidelines have been adapted to take into account the decision handed down by the French Council of State on June 19, 2020.

[2] Deliberation n° 2020-092 of September 17, 2020 adopting a recommendation on the practical procedures for collecting consent concerning cookies and other trackers. See our article entitled The French Data Protection Authority releases a recommendation on cookies published on our Blog in January 2020.