FRENCH DATA PROTECTION: FRENCH SUPERVISORY AUTHORITY PUBLISHES UPDATED GUIDANCE ON COOKIES AND OTHER TRACKING TECHNOLOGIES

Date: 2 October 2020

French Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Laure Comparet, Lucile Rolinet

Following the French Administrative Supreme Court (*Conseil d'État*) dated 19 June 2020 (see our alert here), the French Supervisory (CNIL) published on 01 October 2020 its updated guidelines (the Guidelines), replacing its former guidelines published on 04 July 2019 (July Guidelines), along with practical recommendations (the Recommendation) on cookies and other tracking technologies (together, Cookies).

In line with the revised position from the European Data Protection Board (EDPB—see our alert here), the Guidelines' key takeaways for online services publishers (Publishers) include:

- A case-by-case assessment of the lawfulness of so-called “cookie walls”, which must include in any case information about the consequences of refusing to accept Cookies—this replaces the *ex ante* prohibition from the July Guidelines;
- A characterization of the silence or inaction of the data subjects as a refusal to the setting of Cookies on their terminals; and
- A characterization of entities using Cookies for their own purpose on a given Publisher's website as joint controllers along with that Publisher—which aligns with the recently published EDPB Guidelines 07/2020 on controller and processor and 08/2020 on targeting of social media users.

THE CONDITIONS FOR VALID CONSENT TO COOKIES?

Freely Given

As the cornerstone of consent validity, the freedom to choose between giving or not giving one's consent appeared at odds with the developing practice of Publishers to condition the access to their websites to the prior consent to Cookies (so-called “cookie walls”).

The July Guidelines, which deemed such practices illegal by nature, were reversed on that very issue by the Conseil d'État on the ground that it went above and beyond the letter of the General Data Protection Regulation. The new Guidelines limit themselves to stating that a case-by-case analysis will need to be performed. Yet, the supra-national interpretation of the EDPB leaves little to the imagination on how such analysis will go:

> "In order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls)" EDPB Guidelines 05/2020, Section 39, p. 12

Publishers are therefore advised to stay clear of such practice or, at the very least, to document the rationale behind the need for such cookie walls.

Specific to Given Purposes

Bundling consent with the acceptance of a website's terms of use, or even bundling several unrelated and incompatible purposes would defeat the specificity tenet of consent.

Consequently, Publishers will be required to expose their users to each and every purposes and secure consent for each individually. However, provided that such individual options are made available, nothing would prevent the inclusion of an “Accept All” option as well.

Clear and Concise Information

The Guidelines reiterate the GDPR recommendation to use simple and plain language to inform individuals on the nature and purposes of Cookies, and to avoid legal and technical jargon. In that regard, the CNIL invited stakeholders to come together to devise standardized signalization for the ecosystem. Once again, and in the wake of the Schrems II decision from 16 July 2020 which opened up the way to Codes of Conduct (see our alert here), the CNIL is paving the way for an increased role of self-regulation with regard to Cookies.

The CNIL listed the minimal level information to provide to individuals prior to the request for consent, for it to be valid:

- The identity of the data controller(s);
- The purposes of the Cookies;
- The way to accept or refuse Cookies;
- The consequences of refusal or approval; and
- The right to withdraw the given consent at any time.

The CNL invited Publishers to detail on the first layer of information provided to individuals in a short paragraph:

> "For example, if the cookie is used for customized advertising, the information can be provided in the following way: “Customized advertising: [name of the site/application] [and third party companies/our partners] uses/use tracking devices to display advertising customized to your browsing and your profile."

The thoroughness of that list, along with the clean and simple language and transparency, should lead Publishers to deploy a dedicated Cookie Policy and information notice, separate from a more general Privacy Policy.

Lack of Ambiguity

Unchanged from the July Guidelines and in line with the EDPB, the CNIL refuses to consider that continued navigation through a website could materialize a valid consent. In addition, the CNIL completed this reversal of its pre-2019 position by relying on a Court of Justice of the European Union decision from later in 2019 (CJEU, 01 October 2019, C-673/17, Planet 49), to emphasize that pre-ticked checkboxes could not be construed as valid consent.

But the French Supervisory Authority goes further - while it could have been sufficient to consider that no valid consent would be collected through such means (and that when such prior consent would be required, no processing can be implemented), the CNIL highlights that such silence or inaction should be perceived as a refusal to the setting of Cookies on the user terminal.

Finally, based on the current state-of-the-art, consent cannot be deducted from browser settings since the information provided by the browser itself is not generally sufficient and would not allow users to distinguish between different purposes for the Cookies.

PUBLISHERS AND THIRD PARTIES: FRENEMIES FOR EVER?

The CNIL also seized that opportunity to voice its opinion on the respective roles of each party regarding the setting and storing of Cookies on a user's terminal:

- Publishers using Cookies should be considered as a data controller, even if they rely on a third-party to manage Cookies on their behalf; and
- Other entities (e.g., advertising network) using Cookies should determine their own status regarding the processing implemented on the Publisher's website, either as:
  - data controllers, when using Cookies for their own purposes on third-party websites, such as the Publishers'. In that case, both should be considered as joint controllers and will have to decide how consent may be both received and evidenced by either party; or
  - processor, when using Cookies for the purposes of a third party.
  - In both situations, be it for joint controllers (Article 26 GDPR) or data processor (Article 28 GDPR), specific contractual arrangements will be mandated under GDPR.

With regard to the transparency of the information provided to individuals, the CNIL recommends listing all controllers involved and their roles, along with a link to their privacy policy, to be provided upon the first layer of information of the Cookie banner.

EVIDENCING CONSENT

As part of GDPR's accountability framework, data controllers must be able to evidence that individuals effectively provided valid consents to the setting of Cookies. In addition to the consent-gathering process, individuals' choices will also need to be retained.

The CNIL now recommends that user's choices be stored for a certain amount of time, such amount being determined on a case-by-case analysis depending on the nature of the website or application and on the specificities of the audience and as consent should be renewed at regular intervals.

Previously, the CNIL operated on a 13-month harmonized basis. However, the new recommendation for consent renewal has been lowered to six months, without prejudice to the retention period.

Such renewal process serves a dual purpose: (i) reminding data subjects about the consent they originally provided and confirm it remains valid but also (ii) as a way for Publishers try to obtain a consent which may have been initially denied. The currently widespread consent banner which may come up upon each new visit in case of lack of consent should therefore soon vanish.

In any case, consent should be as easily withdrawn as it has been initially given, at any time and free of charge. To that end, the CNIL recommends using a link to a consent gathering mechanism with a description such as “Management of my Cookies,” “Cookie Management Module” or simply “Cookies”.

CONSENT-EXEMPTED COOKIES: A SILVER LINING?

The CNIL also updated the list of Cookies exempt of consent, as follows:

- Cookies storing the choice expressed by users on their Cookie usage;
- Cookies intended for authentication to a service, including those intended to ensure the security of the authentication mechanism;
- Cookies intended to store a shopping cart on a merchant site or for user billing purposes;
- user interface customization Cookies (e.g., for the choice of language or presentation of a service), when such customization is an internal and expected element of the service;
- Load-balancing Cookies for a communication service; or
- Paywall Cookies, allowing websites to limit free access to a portion of their content (predefined quantity and over a limited period of time);

Regarding analytical Cookies and audience measurement, the CNIL clarified they did not necessarily require the user's prior consent as long as they were solely used to measure the audience of a website or application, provided that such Cookies:

- do not allow the tracking of users across several websites or applications; or
- can only be used to produce anonymous statistical data and the data collected cannot be inferred with other sets of data nor transmitted to third-parties.

When third-party Cookies are used to track the user's navigation beyond the initial site or mobile application, the CNIL emphasized the need for consent to be collected on each of the websites or applications.

Publishers and the AdTech ecosystem have until the end of March 2021 to implement these new requirements and be compliant with them and K&L Gates' French data protection team remains available to assist you during every step of the way.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM