

GDPR, COOKIES, AND THE EVER-FILLING JAR OF EUROPEAN DATA PROTECTION

Date: 26 January 2022

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Camille J. Scarparo

European regulators unofficially announced the major theme of this new year, through the release of several decisions pertaining to cookies and other tracking technologies in the first 10 days of 2022.

As the [General Data Protection Regulation](#) (GDPR) is approaching the fourth anniversary of its entry into force, the [ePrivacy Regulation](#)—a companion piece to address online communication and that was supposed to be adopted at the same time—remains in the limbo of the European legislative process.

In the meantime, the effects of the [Schrems II decision](#) of 16 July 2020 (see our alert [here](#)), which canceled the Privacy Shield and placed stricter requirements on the use of standard contractual clauses, continues to ripple through data protection compliance efforts of companies worldwide.

COOKIES AND DATA TRANSFERS

Subsequent to a complaint filed by None of Your Business ([noyb](#), the aforementioned Maximilian Schrems' association) and in the first decision of its kind, the [European Data Protection Supervisor](#) (EDPS) required the [European Parliament](#) to remediate several breaches of the European data protection framework within a month.

The complaint filed by noyb related to the European Parliament's internal COVID-19 testing website (Website), which allegedly included:

Inconsistent Cookie Banners

A nonexhaustive list describing the cookies placed on users' terminals, as well as discrepancies between such banners depending on the languages of the cookie information notice. The EDPS considered that without detailed information describing all cookies, the necessary cookie consent could not be validly obtained.

Lack of Transparency in the Cookie Information Notice

Vague and unclear data protection notices.

Unclear and Irrelevant Information

The privacy policy was not clear and transparent since it referred either to the processing operations relating to the unrelated COVID-19 testing of the Brussels airport or to a wrong legal basis. During the investigation, the European Parliament changed the policy (possibly to correct the issue), but, arguably, the change made it worse as noyb highlighted additional inconsistencies in the European Parliament's new policy. The EDPS agreed that the policy violated the obligation of transparency, which is a basic legal requirement under European data protection law. Further, the EDPS held that the European Parliament did not adequately reply to the complainants' access request.

Unlawful Transfer Outside of the European Union

The Website relied on U.S.-based service providers, who were the ultimate beneficiaries of the cookies. However, the EDPS found that the European Parliament “provided no documentation, evidence or other information regarding the contractual, technical or organisational measures in place to ensure an essentially equivalent level of protection to the personal data transferred to the US in the context of the use of cookies on the website.” As part of the accountability framework, affected stakeholders must be capable of demonstrating their compliance. Without that documentation, the EDPS concluded that the Website transferred data to the United States without ensuring an adequate level of personal data protection.

This EDPS decision was adopted under [Regulation \(EU\) 2018/1725](#), dated 23 October 2018, which mirrors GDPR's requirements for EU institutions.

COOKIES AND CONSENT

The notoriously cookie-focused [French Data Protection Authority](#) (CNIL) also increased its pressure on cookie management of several companies in two decisions, dated 31 December 2021 (respectively, no. [SAN-2021-023](#) and [SAN-2021-024](#) – links in French), where companies targeted French users for a cumulative fine of €210 million (approximately US\$240 million).

In both cases, the CNIL found that several websites only offered their users the opportunity to immediately accept all cookies, without any possibility to refuse or tailor the cookies used on the sites as easily. Requiring users to take several clicks to refuse all cookies (as opposed to a one-click option) was considered an unlawful hindrance on the “freely-given” requirement for cookie consent.

These decisions are part of the global compliance strategy initiated by the CNIL over the past two years since the revamping of its positions on cookies and other tracking technologies under GDPR (see our previous alerts [here](#), [here](#), and [here](#)) and enacting close to 100 corrective measures (orders and sanctions) against website publishers.

ACTION ITEMS

As a reminder, all publishers with websites or apps that are accessible by a European audience should:

- Have a clear overview of all first- and third-party cookies used on their websites.
- Assess which cookies are (i) strictly essential for the provision of the service, or (ii) nonessential. All analytics or geolocation cookies should, by default, be considered as nonessential absent specific circumstances or special cases.
- Ensure that no cookie is placed on the user's device before providing basic information (a so-called “first layer”).
 - This first layer of information must contain key information about (i) the identity of the publisher, (ii) the purpose of the cookie, and (iii) the rights of the users, and it may be presented in a banner upon accessing the service.
 - A second layer of more specific information should provide additional (and exhaustive) details, notably relating to the cookies' lifespans. In that regard, having a dedicated cookie policy, separate from a privacy policy, is advised.

- When consent is required, include:
 - A graphical user interface using a neutral design.
 - Options to consent or seek more information, along with the ability for the user to indicate if they desire to refuse consent or if they desire to postpone their decision.
 - A consent-gathering mechanism for each purpose.
 - The opportunity for users to withdraw their consent, which may require the deployment of a cookie-management interface.
- Not deny access to the website merely due to the user's refusal to consent (either by ignoring the consent request or by refusal).
- Document both the consent-gathering process and the actual consent-gathering user action as part of GDPR's accountability framework.

K&L Gates [Global Data Protection team](#) (including in [each of our European offices](#)) remains available to assist you.

KEY CONTACTS



CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM



CAMILLE J. SCARPARO
ASSOCIATE

PARIS
+33.1.58.44.15.11
CAMILLE.SCARPARO@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.