French Regulator Imposes Record Fines on Google and Facebook for Cookie Refusal Mechanism Compliance Failure

Date : January 13, 2022

What's this all about?

The French data protection regulator the CNIL (Commission Nationale de l'Informatique et des Libertés) recently fined Google €150 million (around $170 million) and Facebook €60 million (around $68 million) for not making it easy enough for users to reject cookies on the organizations' websites and also ordered them to provide users with a means of refusing cookies that is as simple as the existing means of accepting them. This article is a summary of the decisions and their implications for cookie compliance.

Background – Facebook

The CNIL had received many complaints about how to refuse cookies on the facebook.com website and so in April 2021 it undertook an online investigation into this.

What were the regulator's findings?

The CNIL found that:

- Although there was a button to be able to immediately accept cookies, an equivalent solution (either through a button or another mechanism) was not offered that allowed a user to refuse cookies as easily;
- Instead, it took three clicks to refuse all cookies, as opposed to a single one to accept them, and, further, the button allowing a user to refuse cookies was located at the bottom of a second window and was called "Accept cookies".

According to the CNIL:

- Making the refusal mechanism more complex discouraged users from refusing cookies and encouraged them to opt instead for the ease of the consent button for cookies (in a first window), which affected the freedom of consent of users;
- The information provided was not clear because, in order to refuse cookies, users had to click on a button called "Accept cookies" (displayed in a second window) which necessarily generated confusion and a user may have been led to believe that it was not possible to refuse cookies and that they had no way to manage this;
- Therefore, the methods of collecting consent proposed to users, as well as the lack of clarity of information provided to users, infringed French data protection rules.

What sanctions did the regulator impose?

The CNIL fined Facebook Ireland Ltd. €60 million based on:

- The scope of the processing;
- The number of people affected; and,
- The considerable profits the business made from advertising revenue indirectly generated from data collected by the cookies.

The CNIL also issued an injunction requiring:

- The business to provide Internet users located in France, within three months of the decision, with a means of refusing cookies that is as simple as the existing means of accepting them; and,
- If the business fails to implement this it will be subject to a penalty of €100,000 for every day of delay in

implementing this means of refusal.

Background – Google

The CNIL had received many complaints about how to refuse cookies on the google.fr and youtube.com websites and so in June 2021 it undertook an online investigation into this.

What were the regulator's findings?

The CNIL found that:

- Although there was a button to be able to immediately accept cookies, an equivalent solution (either through a button or another mechanism) was not offered that allowed a user to refuse cookies as easily;
- Instead, it took five clicks to refuse all cookies, as opposed to a single one to accept them.

Therefore, according to the CNIL:

- Making the refusal mechanism more complex discouraged users from refusing cookies and encouraged them to opt instead for the ease of the "I accept" button;
- Therefore, this process affected the freedom of consent of users and infringed French data protection rules as it was not as easy to refuse cookies as to accept them.

What sanctions did the regulator impose?

The CNIL fined Google LLC €90 million and Google Ireland Limited €60 million based on:

- The number of people affected; and,
- The considerable profits the businesses made from advertising revenue indirectly generated from data collected by the cookies.

The CNIL also highlighted that it had already (in February 2021) drawn the attention of the two Google companies to this infringement and also stated that it had communicated on numerous occasions that it should be as easy to refuse cookies as to accept them.

The CNIL also issued an injunction requiring:

- The two businesses to provide Internet users located in France, within three months of the decision, with a means of refusing cookies that is as simple as the existing means of accepting them; and,
- If the businesses fail to implement this they will be subject to a penalty of €100,000 for every day of delay in implementing this means of refusal.

What about One-Stop-Shop?

CNIL said that GDPR's one-stop-shop mechanism did not apply here despite the connections both Facebook and Google had with Ireland. CNIL considered that it was territorially competent to act because the use of cookies were carried out within the "framework of the activities" of the businesses' entities in France which constituted the "establishment" of the businesses' entities outside France, who were jointly responsible because together they determined the purposes and means of using cookies.

Takeaways

This enforcement is part of a general regulatory crackdown that the CNIL has been undertaking for some time now – other regulators may follow suit – and the level of the fines demonstrate how serious cookie compliance failure can be. CNIL says that it has taken action in more than 100 cookies cases since March 2021 when its cookie enforcement campaign began. France is not alone in enforcing cookies laws – we have also seen fines in Belgium

and Spain.

We have also seen quite a bit of litigation over the placement of cookies. We have dealt with a number of litigation threats for clients over the last year or so including from a former claims manager who is threatening widespread cookies litigation.

To manage their cookie compliance risk businesses should consider undertaking an overall cookie compliance audit that may include the following:

1. Identifying cookies that are either operating on or through the website;
2. Confirming what types of cookies they are;
3. Confirming whether cookie ownership is first party or third party;
4. Confirming whether there is any third party access to the cookies;
5. Determining cookie lifespan and deciding whether the duration is justifiable for the stated purpose(s);
6. Confirming the purposes of each of the cookies that are used/intended to be used;
7. Identifying the data that each cookie holds or processes;
8. Confirming if the cookies are linked to other information held about users and whether the use of cookies involves processing personal data;
9. Reviewing consent mechanisms – ask yourself: is it as easy to reject cookies as to accept them? Be especially aware of 'nudging', the colours you use and the look and feel of any cookies banner.
10. Setting out an action plan to address any of the above issues and fully documenting the audit along with updating the business' cookies policy; and,
11. Examining compensation claim risk and having a plan to deal with claims quickly.

Cordery operates a cookies clinic to help with cookies compliance issues – for more details see here: https://www.corderycompliance.com/more-cordery-solutions/cordery-cookies-clinic/.

The French regulator's decisions can be found here: https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros and here https://www.cnil.fr/en/cookies-google-fined-150-million-euros.

We have written about cookies issues including here: https://www.corderycompliance.com/french-regulator-cnil-fines-data-controller-and-data-processor-for-security-breach-sets-deadline-for-cookies-compliance/ and here https://www.corderycompliance.com/cnil-cookies-investigation/ and here https://www.corderycompliance.com/client-alert-eu-privacy-reg-proposed-amends-metadata-cookies-legitimate-interests-consent/ and here https://www.corderycompliance.com/ecj-cookies-consent-ruling/.

We report on data protection issues here: https://www.corderycompliance.com/category/data-protection-privacy/.

We report about compliance issues here: https://www.corderycompliance.com/news/.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com