

C'est la vie? French Regulator Fines Google Nearly \$57 million for GDPR Non-compliance

Alexander I. Schneider

January 25, 2019

On Monday, France's Data Protection Agency [announced](#) that it levied a €50 million (\$56.8 million) fine against Google for violating the EU's new General Data Protection Regulation (GDPR). The precedent-setting fine by the Commission Nationale de l'Informatique et des Libertés ("CNIL") is the highest yet imposed since the new law took effect in May 2018.

How Does Google Violate GDPR, According to CNIL?

- **Lack of Transparency:** GDPR Articles 12-13 require a data controller to provide data subjects with transparent, intelligible, and easily accessible information relating to the scope and purpose of the personal data processing, and the lawful basis for such processing. CNIL asserts that Google fails to meet the required level of transparency based on the following:
 - *Information is not intelligible:* Google's description of its personal data processing and associated personal data categories is "too generic and vague."
 - *Information is not easily accessible:* Data subjects must access multiple Google documents or pages and take a number of distinct actions ("5 or 6") to obtain complete information on the personal data that Google collects for personalization purposes and geo-tracking.
 - *Lawful basis for processing is unclear:* Data subjects may mistakenly view the legal basis for processing by Google as legitimate interests (that does not require consent) rather than individual consent.
 - *Data retention period is not specified:* Google fails to provide information on the period that it retains certain personal data.
- **Invalid Consent:** Per GDPR Articles 5-7, a data controller relying on consent as the lawful basis for processing of personal data must be able to demonstrate that consent by a data subject is informed, specified, and unambiguous. CNIL claims that Google fails to capture valid consent from data subjects as follows:
 - *Consent is not "informed":* Google's data processing description for its advertising personalization services is diluted across several documents and does not clearly describe the scope of processing across multiple Google services, the amount of data processed, and the manner in which the data is combined.

- *Consent is not unambiguous*: Consent for advertising personalization appears as pre-checked boxes.
- *Consent is not specific*: Consent across all Google services is captured *via* consent to the Google Terms of Services and Privacy Policy rather than a user providing distinct consent for each Google personal data use case.

What Does This Mean for Other Companies?

While Google's size, market power, and diversity of offerings (and associated scope of data collection) places it in a somewhat unique position within the online ecosystem, CNIL's action nevertheless offers several practical takeaways for all companies that may be re-assessing their GDPR compliance status in light of this action:

- *Don't Hide the Ball*: Make a concerted effort to ensure that privacy disclosures are clear, easily discernible to consumers, and contain a plain-language description of the categories of personal data that you collect, and the purposes for which you collect it.
- *Minimize Clicks*: To avoid EU regulator scrutiny, reduce the number of clicks required for a consumer to determine the scope of personal data collection relating to your service.
- *Be Upfront on the Legal Basis for Processing*: Explicitly state within your privacy notice your lawful basis for the intended data processing. If you are relying on consent, and your business intends to use the collected data for different purposes, ensure that the consumer has a reasonable opportunity to provide consent for each specific purpose (and avoid pre-checked boxes!).
- *Sweat the Details*: the CNIL action shows that regulators are taking a comprehensive look at how companies are complying with GDPR requirements, including ensuring that consumers understand how long a controller may retain their personal data. Take a checklist approach to GDPR compliance to ensure your privacy disclosures satisfy all requirements.

This week's action against Google is certainly only the first major enforcement action in what promises to be a year that tests the impact and reach of the GDPR. Illustrating that point, just last week, the group [None of Your Business](#), one of two groups that initiated CNIL's investigation into Google, brought yet another lawsuit [accusing Netflix, YouTube, Amazon, Apple, and Spotify](#) of failing to comply with GDPR-mandated access requests.