

LATHAM & WATKINS<sup>LLP</sup>

# Global Privacy & Security Compliance Law Blog

Commentary on Global Privacy and Security Issues of Today

## French State Council Upholds CNIL's €50M Fine for GDPR Violations

By Latham &amp; Watkins LLP on July 2, 2020

Posted in GDPR

***The Council decision contains useful considerations and clarifications on the “one-stop shop” mechanism, transparency obligations, and consent for targeted advertising.***

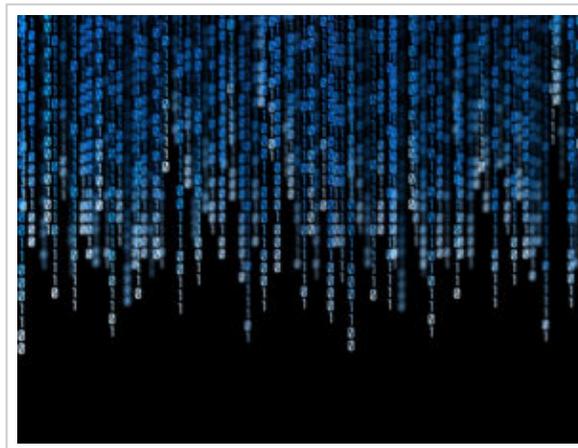
By [Myria Saarinen](#) and [Camille Dorval](#)

On 19 June 2020, France's Highest Administrative Court (Council) handed down its [decision](#) on the appeal filed by Google LLC (Google) against the French Data Protection Authority's (CNIL's) [decision of 21 January 2019](#), which imposed a fine of €50M to Google for failure to comply with the obligations of transparency and to lawfully process personal data on the basis of a valid consent, with respect to the operating system for Android mobile terminals.

### **Additional considerations on the “one-stop shop” mechanism**

In its 21 January 2019 decision, the CNIL found that Google's Irish establishment (Google Ireland) had no decision-making power on the processing operations carried out in Europe in the context of the Android operating system. As a result, the CNIL concluded that the one-stop-shop mechanism was not applicable and that it had jurisdiction over the processing controlled by Google, in the same way as all the other EU supervisory authorities for their respective territories.

In its 19 June 2020 decision, quoting GDPR Article 4(7) and Article 4(16), the Council stated that, for the determination of the lead supervisory authority, the central administration of the controller, *i.e.*, “the place of its actual headquarters”, shall in principle be considered as its main establishment. This shall not be the case “if another establishment of the controller is competent to take decisions on the purposes and means of the processing and has the power to enforce them at the [EU] level”. As a result, if a controller established outside the EU carrying out cross-border processing on the territory of the EU, has neither a “central administration” nor an “establishment



with decision-making powers as to the purposes and means of the processing” within the meaning of GDPR Article 4(16)(a), the “one-stop shop” mechanism provided for in GDPR Article 56 cannot apply.

In its ruling, the Council noted that Google Ireland was Google’s “head office” for its European operations and acknowledged that Google Ireland had “significant financial and human resources”. However, while Google indicated that its Irish establishment was responsible for “numerous organizational functions” for the EU, it did not specify which ones with sufficient details. Thus, according to the Council, the existence of the head office only demonstrated the involvement of Google Ireland in the processing but was not sufficient to show that it had “power of direction or control over [its] EU subsidiaries” to be regarded as a central administration.

Instead, the Council upheld that Google “alone was determining the purposes and means of [the] processing [at stake]” at the time of the investigation and that it had no main establishment in the EU at that time, based on the investigation’s findings that, at the end of 2018 and early January 2019:

- The Android operating system was exclusively developed and operated by Google in the United States.
- Google Ireland did not have any “decision-making power as regards the purposes and means of the processing at stake nor did any of its other EU establishments”.

The Council concluded that no lead authority could be designated under the conditions laid down in GDPR Article 56. As a result, it confirmed that the CNIL had jurisdiction to investigate and sanction the processing carried out by Google concerning French users at the time of the investigation and that the cooperation and consistency mechanism of GDPR Articles 60 to 62 was not applicable.

### **Additional considerations on Google’s failure to comply with the obligations of information and transparency**

Google argued before the Council that its multi-level architecture of the information provided to its users aimed at informing them in a clear and intelligible manner, in line with the recommendations of the European Data Protection Board (EDPB). The first level, consisted of the “Privacy Policy and Terms of Use”, setting out the scope and the main purposes of the processing, while several hyperlinks — “Terms of Use”, “Privacy Policy”, “More Options”, “Rules”, “Learn More” — allowed users access to more comprehensive information.

In line with the CNIL’s prior findings, the Council considered that the dissemination of the information undermined the accessibility and clarity of that information for users, while the processing at stake was particularly intrusive. Specifically:

- The first level of information available to users was excessively general in view of the “magnitude of the processing operations”, their “degree of intrusion into privacy”, and “the volume and nature of the data collected”.
- Key information relating to certain processing operations was accessible only after numerous actions, or only via hypertext links that were difficult to access — for example, the information on the data retention period was only accessible via a hypertext link located on page 68 of the “Privacy Policy”.
- The information provided was incomplete or insufficiently precise, even in the final levels of information — for example, the information on the data retention stated that certain data may be retained “for long periods for specific reasons”, without indicating either the purposes or the data concerned.

### **Additional considerations on Google’s breach of the rules on consent for targeted advertising**

In its 21 January 2019 decision, the CNIL further considered that the consent sought by Google for the placing of targeted advertising was not valid because the information provided was insufficient and the consent was not specific to this purpose only.

In its appeal, Google argued that the GDPR did not require that users give a specific consent for targeted advertising. The Council rejected this argument.

First, referring to the provisions of GDPR Articles 6 and 4(11) and to the judgment of the European Union Court of Justice dated 1 October 2019 (Case *Planet 49*, No. C-673/17), the Council ruled that a “free, specific, informed and unambiguous consent can only be an express consent, given in a fully informed manner after adequate information on the contemplated use of the personal data”.

Then, the Council found that:

- The information provided by Google at the first level of information with regard to the targeted advertising purposes was too general and diluted among other processing whose legal basis was not consent. In addition, consent was collected in a global manner for all the purposes at stake. Therefore the consent sought at the first level was not informed nor specific.
- The information provided at the second level of information was insufficiently complete given the significance of the processing of targeted advertising. In addition, consent was collected by a pre-checked box. Therefore that consent was neither sufficiently informed nor unambiguous (*i.e.*, positively given).

Google argued in appeal that the CNIL had failed to act consistently in at least two manners. First, the CNIL interpreted the requirements on consent that it applied to Google in a manner that substantially derived from the CNIL's previous guidelines adopted in 2013 on the collection of consent for the use of cookies. Second, when the CNIL issued new [cookie guidance in July 2019](#), adopting requirements similar to the one applied to Google, the CNIL decided not to apply these new requirements with immediate effects, but rather to grant a six-month grace period.

The Council rejected both arguments. First, according to the Council, Google could not rely on the CNIL's 2013 cookie guidance, since it was based on Directive 95/46, which was no longer in force at the time of the investigation. Second, Google could not invoke the benefit of the grace period laid down in the 2019 guidance since, according to the Council, the CNIL would have only announced that no sanction would apply during this six-month period if continued browsing was used as a basis for consent. While the Council's first finding seemed convincing, we consider the second one is as far from being clear.

### **Additional considerations on the amount of the sanction**

The Council upheld the amount of €50M considering that the CNIL had provided appropriate motivation to support this amount given the seriousness of the breach at stake, the nature and content of the violated GDPR provisions and their consequences, and the duration of the violations.

The Council noted that:

- In any event, the CNIL has no obligation to include an explanation of the amount of the fine.
- The CNIL is not required to address each of the criteria laid down in GDPR Article 83.
- The CNIL is not required to give a calculation method supporting the amount of the fine.

## Key takeaways

This decision is instructive for businesses for several reasons:

**To benefit from the rules on the lead supervisory authority and the one-stop-shop mechanism**, controllers established outside the EU carrying out cross-border processing in the EU must demonstrate that they have one of the following:

- A central administration in the EU with “power of direction or control over [its] EU subsidiaries”
- An establishment with decision-making powers as to the purposes and means of the processing at stake

**Information provided to data subjects** need not be exhaustive at the first level of information but must be sufficiently precise in any event, especially if the processing operations concern a large number of persons and data and are considered as intrusive. The provision of layered information is possible and even recommended by the EDPB. However, it must not degenerate into a succession of actions to be carried out by the user or into multiple references by hypertext links scattered in excessively long documents. As such, businesses should consider using drop-down menus whenever delivering more precise information is necessary, and using hypertext links only when absolutely necessary and doing so contributes to the clarity of the information. Summary tables are also recommended.

### **When consent is the legal basis of a processing:**

- A specific information notice must be provided at the time of the collection of consent.
- Consent shall not be collected in a global manner for different purposes.
- The use of a pre-checked box shall be proscribed.

**BELJING, BOSTON, BRUSSELS, CHICAGO, DUBAI, DÜSSELDORF, FRANKFURT, HAMBURG, HONG KONG, HOUSTON, LONDON, LOS ANGELES, MADRID, MILAN, MOSCOW, MUNICH, NEW JERSEY, NEW YORK, ORANGE COUNTY, PARIS, RIYADH\*, SAN DIEGO, SAN FRANCISCO, SEOUL, SHANGHAI, SILICON VALLEY, SINGAPORE, TOKYO AND WASHINGTON, D.C. \* IN COOPERATION WITH THE LAW OFFICE OF SALMAN M. AL-SUDAIRI**

---

The purpose of this communication is to foster an open dialogue and not to establish firm policies or best practices. Needless to say, this is not a substitute for legal advice or reading the rules and regulations we have summarized. In any particular case, you should consult with lawyers at the firm with the most experience on the topic. Depending on your specific situation, answers other than those outlined in this blog may be appropriate. Your use of this blog site alone creates no attorney client relationship between you and Latham & Watkins LLP. Do not include confidential information in comments or other feedback or messages left on the Global Privacy & Security Compliance Law Blog Blog, as these are neither confidential nor secure methods of communicating with attorneys.

Portions of this blog may constitute attorney advertising. Any testimonial or endorsement on this profile does not constitute a guarantee, warranty, or prediction regarding the outcome of your legal matter. Prior results do not guarantee a similar outcome. Results depend upon a variety of factors unique to each representation.

Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practices in Hong Kong and Japan. Latham & Watkins operates in South Korea as a Foreign Legal Consultant Office. Latham & Watkins works in cooperation with the Law Office of Salman M. Al-Sudairi in the Kingdom of Saudi Arabia.

STRATEGY, DESIGN, MARKETING & SUPPORT BY

LEXBLOG