Expert Q&A: Lessons from CNIL's EUR50 Million GDPR Enforcement Action Against Google

PRACTICAL LAW DATA PRIVACY ADVISOR

Search the Resource ID numbers in blue on Westlaw for more.

An Expert Q&A with Odia Kagan, Partner and Chair of GDPR Compliance and International Privacy at Fox Rothschild, discussing the CNIL's EUR50 million fine against Google LLC imposed on January 21, 2019. This Expert Q&A focuses on the key issues of the decision, what it means for enforcement, and important implications for companies subject to the GDPR.

On January 21, 2019, the French Commission Nationale de l'information et des Liberties (CNIL) imposed a fine of EUR50 million on Google LLC under the EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR). The decision focuses on the disclosures Google provides to users in France about how it processes their personal data and its legal basis for processing data in the context of personalized advertisements. The fine is the largest fine to date imposed under the GDPR.

Practical Law Data Privacy Advisor asked Odia Kagan, Partner and Chair of GDPR Compliance and International Privacy at Fox Rothschild, to comment on the key findings and implications of the decision and what it means for GDPR enforcement. Odia has assisted more than 80 companies on their path to compliance with the GDPR. She writes regularly on data privacy compliance on the Fox Rothschild Privacy Compliance and Data Security blog.

THE CNIL IMPOSED THE LARGEST FINE TO DATE FOR FAILURE TO COMPLY WITH EU DATA PROTECTION LAWS ON GOOGLE. WHAT WERE THE MAIN ISSUES DISCUSSED IN THE DECISION?

On May 25 and 28, 2018 the CNIL received group complaints from two associations, None of Your Business (NOYB), a not for profit organization founded by privacy activist Max Schrems, and La Quadrature du Net, a French advocacy group promoting digital rights of citizens. NYOB's complaint focused on Android's mobile phone set-up process where users had to agree to Google's privacy policy and terms and conditions to create a Google account and use their device. La Quadrature du Net claimed that Google did not have a valid legal basis to process its users personal data, particularly for ad personalization purposes. The CNIL's investigation reviewed the user journey of creating a Google account on a new Android device and identified two key breaches of the GDPR:

- Lack of transparency, see Transparency.
- Lack of a legal basis for personal data processing, see Consent as a Legal Processing Basis.

TRANSPARENCY

The GDPR requires that privacy notices provide a concise, transparent, intelligible, easily accessible disclosure, in clear and plain language (Article 12, GDPR). The CNIL decided that Google did not comply with the principles of accessibility, clarity, and intelligibility.

While Google's various disclosures contained lots of information about its personal data processing practices, the complicated structure prevented easy access to relevant information. Google scattered key information across several documents which it provided at different times and required users to click multiple buttons and links for additional information to understand exactly how Google planned to use their personal data. For example, accessing relevant information about Google's geo-tracking service required users to take several steps involving up to six positive actions. This made it difficult for users to:

- Easily access and understand important information in its entirety.
- Determine in advance, personal data processing's extent and consequences.

The CNIL also found that Google's vast services, extremely large data collection volume, and processing activity nature combined to make its data processing actions particularly intrusive. However, the information Google provided kept users from fully understanding the extent of Google's processing and what their agreement to continue would permit. For example, the notice:

- Provided generic and vague personal data categories and processing purpose descriptions.
- Failed to clearly state that Google relied on consent instead of legitimate interests for its legal basis to process personal data when personalizing advertisements.

- Never clearly stated how long Google would retain collected information and did not consistently provide data retention periods.

CONSENT AS A LEGAL PROCESSING BASIS

Google relied on consent as the legal basis to process personal data when personalizing advertisements. Valid consent under the GDPR requires a freely given, specific, informed, and unambiguous indication that the data subject agrees to the consent request (Article 4(11), GDPR). The CNIL found that Google failed to obtain valid consent for its processing activities because:

- **The consent request did not sufficiently inform users.** The notice scattered relevant information in different locations and across several documents, making it difficult for users to clearly and fully understand Google's consent request because they had to piece the disparate information together or take several extra actions to access it. For example, the consent request section dealing with ads personalization did not make users aware of the number of services, websites, and applications involved in these processing operations (such as Google search, YouTube, Google home, Google maps, Play Store, and Google Pictures) or the amount of data combined and processed. The user's consent was therefore not sufficiently informed.
- **The consent request was not specific or unambiguous.** To create an account, users had to agree to Google's privacy policy and terms and conditions of use. Google did not seek separate consent for each distinct processing purpose. It instead bundled different types of processing actions together and required users to provide a blanket consent for all of Google's data processing activities using the statement, "I agree to the processing of my information as described above and further explained in the Privacy Policy." The GDPR provides that consent is specific only if it is given distinctly for each purpose. The CNIL held that Google could not rely on this general statement to support its valid consent claim for specific processing actions.
- **Google relied on passive, not active, user action.** By default, Google used personal data for targeting advertisements and required users to opt-out of that use by clicking a "More Options" button and then uncheck pre-checked boxes.

The CNIL took issue with how Google set up the "More Options" button. While users could modify some of their account options through that link, Google pre-checked the account personalization settings by default. It then assumed a user's consent if the person created the account without clicking or reviewing the default settings in the "More Options" link. The CNIL held that if a "More Options" button hides processing activities that require user consent it must:

- Un-check consent grants by default.
- Require that users review and customize the "More Options" component before creating an account.

The GDPR excludes the use of pre-checked boxes.

WHAT ARE THE IMPLICATIONS OF THE DECISION FOR COMPANIES SUBJECT TO THE GDPR?

- **GDPR enforcement is here.** The GDPR grants European Data Protection Authorities (DPAs) power to fine organizations up to 4% of annual worldwide turnover or EUR20 million, whichever is the larger. This fine seems to indicate a willingness to use them. Companies that adopted a wait and see approach should start complying or risk enforcement action.
- **Personalized ads are in the spotlight.** EU DPAs are looking closely at AdTech and behavioural advertising. This is not the first time that CNIL has considered transparency and consent in the context of ad personalization. In 2018, CNIL issued four decisions against small AdTech companies Singlespot, Teemo, Fidzup, and Vectaury, in each case emphasizing the need for clearer transparency and consent.
- **Privacy notices are just that: Notices.** Privacy notices should inform users about how their data is processed. They should not be used to obtain blanket consent. Privacy notices are often too long and complex for users to understand and agree to individual actions in context. Privacy notices should provide easily accessible, concise information that enables users to fully understand the expected data processing's extent. While many DPA's encourage a layered notice approach to improve transparency, organizations must still ensure that users can easily understand core processing activities. This can be a very difficult task, especially when the processing concerns complex activities. As this decision shows, the threshold for what constitutes valid consent is extremely high.
- **Strict requirements for specific and unambiguous consent.** Be as specific and granular as possible when seeking consent. Don't bundle multiple purposes or processes together. The user must be able to consent to specific activities, evidenced by an affirmative action. Statements like "We may use your information for any of the following purposes," do not suffice. Consent requests should not use pre-checked boxes or default acceptance settings.
- **The importance of accessibility.** Ensure users can easily find all relevant information to understand how the organisation plans to process their personal data. A notice should not scatter key information across several documents or require that users click on buttons or links to obtain important information. DPAs generally encourage the use of layered privacy notices as a way of providing clearer information to individuals. However, in this case, Google's structural choices increased the notice's complexity rather than making the information easier to find and understand. Different formats or structures designed to highlight instead of obscure the organization's processing activities may receive a different reception.
- **Consent should not be the default choice.** This decision reinforces the strict requirements for consent. Relying on consent as the legal basis for processing should not be the default choice. The decision did not analyse in detail whether Google could rely on another legal ground, such as legitimate interests, to support its other processing activities.
- **The One-Stop Shop.** Do not assume that establishing an EU headquarters in a particular member state always makes that country's DPA the lead supervisory authority. Instead, the determining factor focuses on where the organization makes decisions about the personal data processing purposes and means. Similar to Google's case, a DPA may conclude that management activity did not occur at the EU headquarters. The more complex the data processing operations, the more complex accurately determining the lead supervisory authority becomes. For more, see What can we learn from this decision about how the one-stop shop mechanism will work in practice?

WHAT CAN WE LEARN FROM THIS DECISION ABOUT HOW THE ONE-STOP SHOP MECHANISM WILL WORK IN PRACTICE?

The GDPR provides a one-stop shop mechanism for companies operating in multiple EU countries. The one-stop shop provides that the DPA in the country where the company has its main EU establishment acts as the lead supervisory authority and assumes primary responsibility for GDPR enforcement. For more on how the one-stop shop operates, see Practice Note, Cross-Border Enforcement and One-Stop Shop under the GDPR (W-016-3325).

Google LLC is a US-based corporation that operates in the EU through an Irish subsidiary, Google Ireland Limited, whose EU headquarters are also in Ireland. The complaints the CNIL received concerned cross-border data processing, which typically triggers the one-stop shop enforcement mechanism under the GDPR. However, the CNIL (and not the Irish DPA) imposed the fine against Google LLC.

The CNIL determined that although Google LLC has EU headquarters in Ireland, Google's US headquarters made the data processing decisions in relation to the purposes and means of the relevant cross-border data processing activities, not Google Ireland or any other EU entity. The CNIL relied on the following factors to support its decision:

- Google's privacy policy does not mention Google Ireland Limited as the data controller.
- Google Ireland Limited had not appointed a data protection officer to oversee Google's EU processing operations.
- Google LLC solely developed the Android operating system.
- Google indicated to the Irish DPA that the transfer of responsibility of Google LLC to Google Ireland Limited on certain processing of personal data concerning EU citizens was to be finalized on January 31, 2019.

For these reasons, the CNIL determined that it was competent to act because the one-stop shop did not apply. The UK ICO has followed the CNIL's decision by announcing similar enforcement action against Google.

This decision highlights the complexity around identifying a lead authority and that regulators will independently assess their authority to act based on the processing actions at issue instead of merely relying on a physical EU headquarters location. Organizations should consider the following:

- How to structure decision-making functions throughout the organization. Where different legal entities within an organization are responsible for making data processing decisions, the organization may have to deal with multiple lead supervisory authorities for different processing activities. This renders the benefits of having one lead authority moot.
- Companies subject to the GDPR, but established outside of the EU, cannot participate in the one-stop shop mechanism. This opens them up to enforcement actions from multiple supervisory authorities. Companies should consider if setting up an EU establishment benefits the organization for the purposes of EU enforcement and co-operation with EU DPAs.
- Document the company's main establishment for the purposes of determining the lead supervisory authority. One reason the CNIL refused to recognize the Irish DPA as Google's lead supervisory authority was the failure of Google's privacy policy to identify Google Ireland Limited as the entity responsible for personal data processing decisions in the EU. Companies with EU locations should actively identify their main establishment to take advantage of the one-stop shop mechanism and avoid the risk of multiple enforcement actions.

WHAT IMPACT COULD THIS DECISION HAVE ON THE FUTURE OF TECHNOLOGY AND AD PERSONALIZATION?

The CNIL decision requires companies that process personal data to profile and target individuals to review certain aspects of their operations or risk enforcement. This has already started happening. For example:

- A large newspaper recently moved to contextual and geographical advertising in Europe with no adverse effects to revenue.
- AdTech companies Fidzup, Singlespot, and Teemo revised their privacy notices and their consent process to be more specific and informed after receiving CNIL enforcement notices.
- The Interactive Advertising Bureau (IAB) stated that it will review its consent management platform and guidelines to align it with GDPR requirements after the CNIL issued its decision against Vectaury. Initiatives such the IAB Tech Labs PrivacyChain are looking for alternative solutions to manage consent which meets the GDPR's high standards.

DOES THIS DECISION ILLUSTRATE HOW WE CAN EXPECT REGULATORS TO ENFORCE THE GDPR?

It was only a matter of time before an EU regulator used its new powers to issue large fines and is not surprising that a multinational tech giant was the recipient. The CNIL justified its decision to fine Google EUR50 million based on:

- The severity of the breach.
- Infringement of core concepts of consent and transparency.
- The fact that the breaches were ongoing, the number of people affected, the volume of data and the level of intrusion.
- The dominant position Google holds in the operating system market.

These attributes are more common in large multinational corporations.

The CNIL's large fine represents a clear statement that it expects compliance with the GDPR's high standard, particularly around the core principles of transparency and consent, and continues a trend of enforcement actions in this area. Regulators have repeatedly warned about online behavioral advertising, automated profiling, and invisible processing by third parties. The issue of how to provide users with meaningful information and control, especially where the underlying processing operations are complex and involve multiple players is particularly challenging in data heavy industries and will likely be the subject of future enforcement. This is only the first fine and we can expect more.

Despite the potential for large fines, EU DPA's have made it clear that fines are only one method of enforcement. They also have other enforcement tools, such as the power to issue injunctions or orders to stop processing personal data, which may cripple an organization.

An organization that demonstrates its intent to comply with the GDPR and cooperates with regulators to address deficiencies may avoid significant fines. Large fines will generally be reserved for organizations that repeatedly breach the GDPR and engage in invasive data processing activities. While a large company like Google, with annual turnover over EUR96 billion, can easily manage the objectively high EUR50 million fine, it still represents a strong warning sign.

GOOGLE HAS ANNOUNCED IT WILL APPEAL THE DECISION. CAN YOU EXPLAIN HOW THE APPEAL PROCESS WORKS?

The size of the fine and the significance of the decision to online advertising revenues and certain business models meant Google's appeal of the decision was inevitable. Google has invested significant resources to comply with GDPR requirements and is concerned with the far-reaching implications of the decision on publishers and tech companies.

The French Supreme Administrative Court (Conseil d'Etat) will hear the appeal and may decide to refer some of the questions to the European Court of Justice. The appeal may provide further insight on what constitutes transparency and consent in the context of personalized ads. The appeal could change any aspects of the decision. It could reduce the fine or increase it. If Google loses the appeal, it must change its privacy notices and how it obtains consent to meet CNIL's requirements.

The practices used by Google are commonplace and so the outcome of the appeal is of interest to many.

For more on enforcement under the GDPR generally, see Practice Notes, GDPR and DPA 2018: enforcement, sanctions and remedies (UK) (W-005-2487) and Cross-Border Enforcement and One-Stop Shop Under the GDPR (W-016-3325).

04-19