

Business Adjusts to Data and Privacy Rules

April 2019



**Bloomberg
Law®**

Informed Consent Will Be Key Privacy Issue

By Lisa Singh

The largest regulatory fine leveled against a company since the General Data Protection Regulation was enacted in May 2018 is poised to reshape business compliance practices across industries.

In late January, CNIL fined Google nearly \$57 million, citing what the French data-protection regulator saw as failure to meet the core requirements of informed consent under GDPR. As Google appeals the decision, as confirmed by a company spokesperson to Bloomberg Law, the debate is far from settled about what constitutes informed consent in personal data collection.

"The notion of informed consent is essential to the success of any privacy regime," said Elizabeth Banker, vice president and associate general counsel at the Internet Association. "However, CNIL's opinion doubles down on a consent model that may result in over-notification of consumers without delivering better privacy protections."

A pre-ticked box requiring no affirmative user action was ruled invalid consent, according to Bloomberg Law.

Google maintained that its pre-ticked "I agree" boxes sufficiently covered user agreement across the myriad data processing activities that underpin advertising personalization. CNIL, however, held that the notification failed to follow the "essential principles" of consent – freely given, specific, informed, and unambiguous.

The ruling holds far-reaching implications for companies whose revenue is driven by personalized ads. In reassessing online behavioral advertising practices, experts said, companies face a conundrum.

"On the one hand, they are being told their policies must be clear and concise," said Daniel Castro, vice president of the Information Technology and Innovation Foundation. "On the other hand, they are being told their policies must be complete and comprehensive."

Given the balance of obtaining valid consent and complying with the right of consumers to withdraw agreement at any time, legal experts advise sidestepping the need for informed consent wherever possible.

"The key lessons from the decision are, first and foremost, that consent is a high-risk lawful ground to process personal data and should only be used [as] a last resort where no other lawful ground is available," said Ross McKean, partner in DLA Piper's London office and co-chair of the firm's data protection practice.

McKean cites the GDPR's inclusion of various "other lawful grounds" for gathering personal data, such as where processing is necessary for performing or entering into a contract, or where processing is in the legitimate interests of the controller, or a third party – "provided these are not overridden by the rights and freedoms of the data subject."

This assessment may take on greater weight, experts said, as action by other organizations gathers steam. The CNIL decision came after two associations – privacy activist Max Schrems' Vienna-based NOYB (short for, "None of Your Business") and the French nonprofit La Quadrature du Net – lodged complaints about Google's processing of personal information. Other consumer advocacy groups are expected to follow suit.

"Although global technology companies are likely the initial and primary targets of their complaints, all industries are exposed to their [consumer groups'] newfound powers under GDPR," said Rita S. Heimes, general counsel and research director of the International Association of Privacy Professionals.

Beyond cementing consumer advocacy groups' right to advocate for data subjects, the CNIL decision places limits on GDPR's one-stop-shop mechanism. The intent of OSS was to allow organizations engaged in cross-border data processing to have claims reviewed by a single data protection authority based on the location of the data controller's "main establishment" in the EU.

Google argued that its main establishment was in Ireland, suggesting the case be brought before the Irish Data Protection Commission, but CNIL stated the office had no decision-making authority over Google's data processing operations. This strict interpretation of a "lead supervisory authority" by CNIL also merits corporate consideration.

All industries are exposed to consumer groups' newfound power under GDPR.

"This may mean that just appointing a representative – or even having an office in the EU – will not necessarily trigger one-stop shop," Heimes said.

In the meantime, businesses need to proceed with caution, ITIF's Castro said. "Companies should know that European regulators are paying close attention to complaints and not letting off first-time violators with just a warning. Any violation can result in a serious fine."

Nor will the scythe cut only the tallest grass. Beyond Google, CNIL leveled a fine against a French startup in October. Companies large and small are on notice.

"The CNIL decision is a wake-up call to review existing privacy policies, cookie notices, and banners to ensure that consents are specific and informed," McKean said.

For general counsel, "the most important step is to understand not only all of their organization's data processing activities, but the lawful basis for each one," Heimes said.

"If consent is the only appropriate basis for an activity, counsel should make sure [it] is acquired through a clear and affirmative opt-in statement, with no pre-ticked boxes, accompanied by a simple statement of what the consent is for, with mechanisms in place to track the consent and allow for its withdrawal," Heimes said. "Vague and generic statements will not suffice."

Lisa Singh is a writer specializing in business and technology matters.



**Bloomberg
Law[®]**

© 2019 The Bureau of National Affairs, Inc.