KUTAKROCK

January 22, 2019

France Fines Google €50M for Alleged GDPR Violations

On January 21, 2019, France's National Data Protection Commission ("CNIL") announced a €50M fine against Google under Europe's General Data Protection Regulation (GDPR).[1] CNIL's press release and Deliberation No. SAN-2019-001[2] provide crucial insights into the first major fine imposed under the new data protection regulation since it went into effect in 2018.

Alleged Breaches

CNIL "observed two types of breaches of the GDPR." First, CNIL alleged that Google breached its transparency and information obligations under Articles 12 and 13 of GDPR. In simple terms, the CNIL determined that the disclosures required under those Articles were made, but that they were not readily accessible by Google's users in an understandable way. Specifically, CNIL called out Google's decision to spread the required disclosures across multiple linked documents, including a Privacy Policy, Terms of Use, and a "Rules of Confidentiality" document, which required the user to engage in cross-checking and "multiplied the clicks necessary" in order to access the information. CNIL pointed out that two such disclosures required at least five clicks in order to access the information immediately relevant to the user. CNIL also seemed to imply that Google's transparency obligations were heightened by the high quality of the personal data it holds on its users. In sum, CNIL found that the user was not able to accurately measure the scope of Google's processing and its effects on the user's private life from Google's privacy policy.

Second, CNIL found that Google lacked a lawful basis to process the personal data at issue. Google designated consent as its lawful basis for processing under its privacy policy. GDPR specifies that consent must be freely given, specific, informed, unambiguous, and indicated by a statement or clear affirmative action.[3] It also imposes a positive obligation upon a controller that relies on consent as its lawful basis to demonstrate that consent, and includes a number of technical requirements for the consent itself.[4] Google argued that the privacy policy fulfilled those requirements. CNIL determined (1) that the user was not sufficiently informed because of the deficiencies identified in the first breach, (2) that the consent was not indicated by a clear affirmative action because a user could finish creating her account without viewing the information contained under "More Options" within the dialogue, and (3) that ticking a checkbox did not sufficiently signify acceptance of Google's terms and conditions of use because it was a single indication of acceptance for multiple purposes of processing, and because the boxes under "More Options" were pre-checked. CNIL also found that Google had not

---

[1] CNIL, *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, January 21, 2019, https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[2] CNIL, *Délibération de la formation restreinte n° SAN – 2019-001 du 21 janvier 2019 prononçant une sanction pécuniaire à l'encontre de la société GOOGLE LLC*, January 21, 2019, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552.

[3] GDPR Art. 4(11).

[4] GDPR Art. 7.

complied with various rules in CNIL's own recommendations and the ePrivacy Directive with respect to cookies.

One-Stop-Shop Mechanism

This enforcement action is also the first test for the outer limits of GDPR's "one-stop-shop mechanism." In general, the supervisory authority of the country in which a controller or processor is established (that entity's "lead" supervisory authority) is charged to enforce GDPR against that entity and coordinate enforcement among any other "concerned" supervisory authorities.[5] An exception provides that a supervisory authority in another country may address alleged violations by that entity if (a) "the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State" and (b) the lead supervisory authority declines to handle the case after being properly notified.[6] GDPR provides a procedure for coordination among those multiple supervisory authorities,[7] but specifies that the lead supervisory authority "shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."[8]

According to the Deliberation, Google argued that the one-stop-shop mechanism meant that only the Irish supervisory authority would be competent to enforce GDPR in this way. In keeping with the European Data Protection Board's latest guidance on this question,[9] the CNIL looked to the decision-making authority actually vested in Google's Irish headquarters in order to determine whether it qualified as a principal establishment. CNIL found that Google Ireland Limited would not have had any decision-making power with respect to the purposes and means of processing covered by the privacy policies that were the basis of these complaints. It pointed to a few critical facts as evidence for that determination: (1) that Google did not designate Google Ireland Limited in its applicable privacy policy as the entity with that authority, (2) that Google Ireland Limited did not appoint a data protection officer who would be in charge of that processing, (3) that Google LLC was solely responsible for the development of the Android operating system, (4) that Google acknowledged a transfer of responsibility for such processing from Google LLC to Google Ireland Limited that was to take place by January 31, 2019, and (5) that the Irish supervisory authority had publicly denied that it was the lead supervisory authority for Google's European operations. CNIL therefore determined that the one-stop-shop mechanism did not apply and that it was competent to handle the complaints.

Fining Authority

This enforcement action is the first fine issued by a supervisory authority that seeks to take advantage of the 4% of annual turnover upper limit allowed under GDPR. CNIL argued in the Deliberation that the fine was appropriate because Article 6, which defines the acceptable lawful bases for processing, is "central" to GDPR as a whole, and because transparency and disclosure requirements are among those punishable by the greatest fines under Article 83(5). This fine may not pose an existential threat to one of the world's largest companies, but it could easily do so for smaller organizations engaged in similar processing and disclosure practices.

Advocacy Groups

Finally, this enforcement action validates Max Schrem's None Of Your Business ("NOYB") advocacy group and its sister entity, La Quadrature du Net, as non-profit associations competent to act on behalf of their member data subjects under Article 80 of GDPR. The alleged violations were brought to CNIL's attention in

---

[5] GDPR Art. 56(1); WP244.
[6] GDPR Art. 56(2-5).
[7] GDPR Art. 60.
[8] GDPR Art. 56(6).
[9] European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) - Version for public consultation*, adopted November 16, 2018.

complaints[10] filed by these two groups immediately after GDPR came into force on May 25 and 28 of 2018. The Deliberation sets out the entire proceeding in fuller detail, including the various reports, comments, and replies from CNIL to Google and vice versa. Companies that engage in similar processing, especially those that rely upon consent as their lawful basis for doing so, should closely monitor those groups and their other complaints in order to stay ahead of enforcement activities by supervisory authorities in France and other European countries.

Kutak Rock's Privacy and Data Security Practice Group regularly advises U.S. and multinational clients with respect to GDPR compliance and enforcement. The Practice Group has closely monitored all major guidance and enforcement activity since well before GDPR's effective date, and stands ready to assist clients that wish to improve their risk posture with respect to this expansive regulation.

Please contact a member of our Privacy and Data Security Practice Group listed below. For more information concerning our privacy and data security practice, please visit us at www.KutakRock.com.

Contacts

Nicole Moriarty	Washington, DC	(202) 828-2446	Nicole.Moriarty@KutakRock.com
Jon Breyer	Minneapolis	(612) 334-5057	Jon.Breyer@KutakRock.com
Jacob Tewes	Omaha	(402) 661-8611	Jacob.Tewes@KutakRock.com

[10] noyb NEWS, *GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook*, May 25, 2018, https://noyb.eu/4complaints/.