DE BRAUW
BLACKSTONE
WESTBROEK

First big GDPR fine for Google: implications for multinationals

On 21 January 2019, the French Data Protection Authority CNIL imposed a EUR 50 million fine against Google LLC for violating the EU General Data Protection Regulation (GDPR). As the first enforcement action in Europe that resulted in a large fine under the GDPR, the CNIL decision is the first step on a long trial-and-error path of GDPR enforcement by Data Protection Authorities ("DPAs"). The CNIL investigation is sure to become a landmark case in Europe, as Google has already stated that it will appeal the decision in court.

CNIL conducted the investigation at breakneck speed and fined Google immediately, even though Google requested that CNIL impose a compliance program instead. CNIL neither completely explained why the fine was imposed so quickly nor did it provide the reasoning for the amount of the fine. Moreover, it explicitly sidestepped the one-stop-shop mechanism that allows multinationals to designate one "lead" authority for Europe to alleviate compliance and enforcement burdens. This has serious implications for multinationals, which should now take immediate steps to prepare themselves for a new era of privacy enforcement and assess their appetite to appeal against enforcement decisions by DPAs in court.

CNIL's investigation against Google

CNIL's investigation was triggered by the complaints of two NGOs, which coincided with the coming into force of the GDPR on 25 May 2018. CNIL found Google in violation of two core obligations under the GDPR: the obligation to be transparent about personal data processing activities to customers, and the requirement to have a legal basis for such. On the first count, CNIL concluded that Google did not provide Android users with comprehensive, clear and consistent information about the processing of their personal data. On the second count, CNIL deemed the consent on which Google relied in using European citizens' personal data for personalisation and targeted advertisement, invalid. Such consent, according to CNIL, was not sufficiently "informed", or "specific" and was "unambiguous". In particular, CNIL underscored the fact that the GDPR requires companies to obtain a separate consent for each specific purpose of processing. CNIL held that Google did not ask users to consent to personalisation and instead obtained general consent for all data processing under its Privacy Policy.

One-stop-shop mechanism does not apply equally to all multinationals: a potential violation of international trade law commitments

CNIL decided that the one-stop-shop mechanism did not apply in this case. The mechanism

is a GDPR novelty and allows multinationals to select one "lead" DPA across Europe. In theory, companies should only have to deal with this "lead authority" in enforcement actions in Europe. The "lead" DPA then has to coordinate with other relevant DPAs across Europe through a consistency mechanism.

This did not work out for Google. CNIL found that Google LLC transferred the responsibility for processing European citizens' data to Google Ireland only on 3 December 2018, when CNIL's enforcement action was already in full swing. Google's Privacy Policy did not identify the main establishment in charge of decision-making regarding the purposes and means of data processing in the EU. In addition, Google Ireland, which Google claimed to be its main establishment before CNIL, did not appoint a Data Protection Officer ("DPO") to oversee all personal data processed in the EU.

Therefore, CNIL held that Google LLC did not have a "main establishment" in the EU, which is used as a benchmark in determining the "lead" DPA. Consequently, CNIL argued that the one-stop-shop principle did not apply. The consequences are serious: disregarding that Google had selected the Irish DPA as the "lead" DPA, CNIL claimed jurisdiction over the case and immediately issued the first multi-million fine under the GDPR.

CNIL's approach creates differential treatment of companies that make all data processing decisions in the EU and non-EU companies making such decisions outside the EU. This raises the critical question of whether this GDPR interpretation complies with the EU's international trade commitments under the law of the World Trade Organization (**"WTO"**). Under Article XVII of the General Agreement on Trade in Services, the EU must grant foreign services and service providers no less favourable treatment than similar domestically-produced services and their providers (national treatment). Personal data processing services are among the sectors to which national treatment applies. CNIL sets a threshold that is almost impossible to satisfy for non-EU companies. Therefore, the risk of a WTO law violation may be more real than it may seem. Focusing solely on the GDPR, European DPA's seem to overlook the broader relevance of their practices.

The ambiguity around the calculation of the fine

CNIL's decision is the first where an administrative fine for GDPR violations was calculated based on the undertaking's worldwide turnover. The notion of "undertaking" has been borrowed from competition law. According to the CJEU, in contrast to a "legal entity", an "undertaking" means an economic unit, which may be formed by a parent company and all subsidiaries involved.

CNIL does not offer any explanation or methodology for determining the high amount of the administrative fine, EUR 50 million, which seems to have been produced out of thin air.

As we predicted, this decision is only the first step on the long and winding road of determining such methodology. In relation to the choice of a fine as a corrective measure (instead of a binding instruction coupled with a potential sanction), CNIL mentioned that the use of personal data for profiling and Google's business model were among decisive factors. CNIL also highlighted Google's prominent position in the market, but did not include competition law concerns in its analysis.

GDPR: enter the enforcement and litigation era

Expected by many, feared by some, CNIL's decision marks the arrival of GDPR enforcement.

Clearly, CNIL had an interest to proceed fast with its investigation, as Google was already preparing to move its main establishment to Ireland. By moving (too?) quickly and boldly, one wonders whether CNIL's reasoning will hold up in court.

Google has announced it will appeal against the decision. If the trend of bold DPA decision-making continues, a new era of privacy litigation between companies and authorities is upon us. This is not unlike the explosion of litigation around access conditions to telecommunications infrastructure in the 1990s.

Takeaway: "main establishment" requires financial and organisational investments

Before a myriad of regulators knock on their doors, multinationals should move fast: it is imperative to (re)assess which European establishment qualifies as a main establishment, and to identify a "lead" supervisory authority accordingly. This main establishment should be appointed both internally and in external privacy policies. Moreover, the designation of the main establishment should be backed by necessary financial resources and actual decision-making powers. If companies are under the obligation to appoint a DPO, the DPO should be based in the same location. Naturally, it is also important to review the structure and availability of information on personal data uses and related consent request mechanisms.

Companies that do not move quickly on these issues risk an onslaught of investigations across Europe, by DPAs – such as CNIL – that do not shy away from bold enforcement actions.

For further analysis, please read Axel Arnbak's article in Dutch financial newspaper Het Financieele Dagblad here.