SROUJI AVOCATS
AVOCATS À LA COUR

www.sroujiavocats.com

Rethinking the notion of main establishment under the GDPR: the Google case

April 2019

Célia Tellaa, Avocate à la cour
Joseph Srouji, Avocat à la cour

Much has been written about the recent decision by the French *Commission Nationale de l'Informatique et des Libertés* (CNIL) earlier this year, fining Google 50 million euros for various GDPR violations (currently under appeal).

Apart of the classic regulator grievances — lack of transparency and difficulty navigating disjointed privacy policies and deciphering notices to obtain freely given and unambiguous consent – there was some surprise regarding as yet unchartered territory under the GDPR: designating a lead Supervisory Authority – the "one-stop-shop." Companies in theory should be able to designate a lead Supervisory Authority in the jurisdiction where its main establishment is located.

In the case of Google, the company clearly miscalculated in its interpretation of where its main establishment was located, and hence overestimated its ability to anticipate and manage regulatory action from a single regulator located in the jurisdiction of its choosing.

What the GDPR says about main establishment: reading between the lines

The question of Supervisory Authority competency arises when a dispute involves cross-border data processing. Article 4 (23) of the GDPR[1] defines this as situations where a company is established in more than one EU member state and processes personal data in one of those states. This also includes situations where a company is established in one member state and

[1] (23)' cross-border processing' means either:
(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or
(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

processes data in this same state but that processing has substantial effects on another member state.

Articles 55 to 67 of the GDPR address the issue of a conflict of jurisdictions by providing for a lead Supervisory Authority system. The advantage of this system is that companies can focus their energies on a single Supervisory Authority (ideally one of their choosing), which is competent to address complaints or queries potentially arising in EU jurisdictions other than that of the lead Supervisory Authority.

International companies with pan-European operations, sometimes with multiple EU-based business unit headquarters, have grappled with the question of which EU member state Supervisory Authority would be the most appropriate. The analysis is in no doubt influenced by a company's perceptions of a regulator's enforcement stance and pro-business attitude.

While there is relatively rich jurisprudence on the question of "establishment" (both in data protection and in competition law), Article 4 (16) of the GDPR[2] defines "principal establishment" as the place where the company has its central administration in the EU unless the decisions regarding processing personal data are taken in another establishment which has the power to have those decisions implemented. This definition, however, does not necessarily consider the complexities of how some international groups operate in the EU – a crucial point in which Google unfortunately fell victim.

The former Article 29 Working Party (now the European Data Protection Board or "EDPB"), in its White Paper 244 of April 2017, interprets this provision as the possibility for a company to determine with precision the place where decisions are taken. One of the criteria in determining main establishment includes the designation of a Data Protection Officer (DPO) in the desired jurisdiction.

In regards to a group of companies, the EDPB interprets broadly, considering that the main establishment is that of the jurisdiction where the headquarters (exercising authority over the other group entities) is located.

In the case of joint data controllers, the EDPB relies on Article 26 and Recital 79 to determine that the joint data controllers, in this situation, should transparently define their respective obligations and designate the establishment having the power of making final decisions in regards to data processing.

---

[2] 'main establishment' means:

a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;

b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation;

Things get more complicated, and risky for companies like Google, when it comes to cases in which it is not clear which EU member state has decision-making authority. In this scenario data controllers are located in various EU member states but no single entity can be identified as the main establishment. The GDPR does not explicitly address this point and the EDPB is of the opinion that no lead Supervisory Authority can therefore be designated, and that a regulatory investigation could be led by one or more Supervisory Authorities. This is the scenario that Google confronted.

Where the Google case stands out is that, for reasons explained below, Art. 65 of the GDPR was not considered by the CNIL. It reads:

"(1) In order to ensure the correct and consistent application of this Regulation in individual cases, the [European Data Protection] Board shall adopt a binding decision in the following cases:
b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment"

No luck of the Irish for Google

Complaints against Google originated in May 2018 from the groups "None of Your Business" ("NOYB") and *La Quadrature du Net* ("LQND") – the latter representing about 10,000 concerned individuals. The CNIL initially took the lead and submitted the complaints in June 2018 to all EU Supervisory Authorities with the intent to identify the appropriate lead Supervisory Authority.

After discussing with its counterparts and more particularly with the Irish DPA, the CNIL concluded, with the help of an *in concreto* assessment, that the elements provided by Google regarding the designation of the Irish DPA as its lead Supervisory Authority, in the end revealed the capacity of Google Ireland Limited to make decisions regarding different activities of the company (financial and accountability, contracts etc.) but not regarding personal data processing.

Also, Google's privacy policy did not indicate its Irish entity as the "deciding" entity on data processing activity. In addition (and most foolishly for Google), the Irish Google entity did not bother to designate a DPO in charge of the management of personal data processing across the European Union. In terms of Google's technology, the CNIL pointed out that the Android operating system is developed exclusively by Google LLC (the US entity). In a curious last-minute manoeuvre by Google, the CNIL refused to recognise a letter sent by Google US to the Irish Supervisory Authority claiming to have "transferred" specific data processing responsibilities to its Irish entity – effective 22 January 2018 (the CNIL levied the fine on the 21st!).

As a result, the CNIL took the position that no main establishment could be determined for Google in the EU, allowing it to essentially assume the role of lead Supervisory Authority,

being competent therefore to manage complaints according to Article 58 (2) (i)[3] and levy a fine according to Article 83 of the GDPR against the Google LLC (US) via its French subsidiary.

Needless to say, this solution was not at all to Google's liking. Google challenged the CNIL with regard Article 65 of the GDPR and the requirement to call upon the EDPB whenever a conflict occurs between different Supervisory Authorities to determine main establishment. The CNIL pointed out that the Irish Supervisory Authority confirmed publicly in the *Irish Times* that Google was subject to all European Supervisory Authorities and not specifically to the Irish one – no conflict was therefore characterised in the eyes of the CNIL.

Comments

It does not appear in this case that the CNIL runs afoul of the GDPR nor the interpretation of the GDPR by the EDPB. Here, the CNIL considered that the lead Supervisory Authority system was not applicable. In other words, the CNIL, by querying the other Supervisory Authorities on lead Supervisory Authority and by having received a negative answer, concluded that there was no conflict of jurisdiction and no rule of competency to evoke. This way, the lead Supervisory Authority system was not effective and the CNIL therefore considered itself competent acting on behalf of France.

When justifying its sanction, the CNIL added:
"The limited training reminds us that the company is implementing data processing on a considerable scale given the predominance of the Android operating system **on the French market** for mobile operating systems and the proportion of telephone users **in France** who use computers. Thus, the data of millions of users are processed by the company in this context."

This sanction only applies to actions Google took on the French market and against French users. However, Google of course operates globally, which means that this could only be the beginning of its worries – additional fines could conceivably be levied by other Supervisory Authorities regarding other markets in Europe.

To mitigate this risk, Google has modified its privacy policy and plans to transfer its data processing responsibility from Google LLC (US) to Google Ireland Limited.[4] This should indeed calm regulatory nerves and provide some certainty that the Irish Supervisory Authority is indeed Google's main Supervisory Authority. But this would not prevent the Irish Supervisory Authority from levying fines on behalf of all EU regulators (potentially reaching 4% of Google's worldwide turnover).

Google appealed the decision to the French *Conseil d'Etat* (Supreme Court for administrative matters), but it is entirely feasible that the matter will be heard before the European Union

[3] Each supervisory authority shall have all of the following corrective powers:
(i) to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case;

[4] Nathalie Maximin, *Application du RGPD par la CNIL : précisions et amende record pour Google,* 28 janvier 2019, Dalloz actualité

Court of Justice. This would be a positive development since it would provide some precedent to help other companies better draw the line when it comes to determining main establishment in regards to their data processing activities.