Client Alert: French Data Protection Authority Fines Google €50m for violations

Date : January 22, 2019

https://youtu.be/sj2_3s-BicI

Introduction

Yesterday's €50m GDPR fine from the French Data Protection Authority shows that GDPR isn't just about data security. The case underlines the importance of transparency under GDPR and also has important pointers for the way in which other parts of GDPR will work, including the one-stop-shop mechanism.

This note includes some technical data protection terms which are explained in our glossary here www.bit.ly/gdprwords. For background to GDPR see our FAQs here www.bit.ly/gdprfaq

What is the background to the case?

The case concerns two of the first complaints filed under GDPR in May 2018. The first set of complaints was received just after GDPR came into force on 25 May 2018 from Max Schrems and his pressure group None Of Your Business (NOYB). You can find out more about Mr. Schrems and his views on privacy in our interview with him here http://www.corderycompliance.com/interview-with-max-schrems/. The NOYB complaints were followed on 28 May 2018 by complaints from a French pressure group, La Quadrature du Net (LQDN). LQDN said that it was making its complaint on behalf of 10,000 data subjects. The complaints were made to the French Data Protection Authority, Commission Nationale de l'Informatique et des Libertés (CNIL).

What were the complaints about?

Both NOYB and LQDN complained that Google did not have a valid legal basis to process the personal data of users of its services, particularly for the personalisation of advertising. They complained about 'enforced consent' i.e. consent which is not freely given since there is no other option if you want to use the services offered.

What did CNIL do?

CNIL seems to have initially tried to deal with the complaints under the so-called one-stop-shop mechanism. One-stop-shop was sold to businesses as one of the key elements of GDPR allowing an organisation (in principle at least) to deal with just one EU Data Protection Authority (DPA) for complaints across the EU. Under GDPR national independent regulators remain in place. To enable a business to deal with just one DPA, under GDPR, the DPA of either the main establishment, or, (if this is the case) of the single establishment of a data controller or data processor, will act as lead DPA where data processing carried out by that data controller or data processor is cross-border – i.e. it cuts across EU Member States. A special EU co-operation procedure between DPAs applies in these cases. There's quite a complicated system in place to work out who the lead DPA will be. This is not something that an organisation can select for themselves. There is a more detailed guidance note on one-stop-shop in GDPR Navigator (see www.bit.ly/gdprnav).

On 1 June 2018 CNIL sent these two complaints to other EU DPAs as part of the one-stop-shop process. CNIL says that it held discussions in particular with the Irish DPA but said that since the Irish Google presence did not at the time have decision-making powers for the processing operations in question for Android devices one-stop-shop did not apply. As a result CNIL could launch its own investigation. CNIL also says that any other EU DPA can also launch its own investigation too and, presumably, also has the power to issue its own fine. CNIL started some online investigations in September 2018.

Breaches of GDPR

In essence CNIL says that there are two breaches of GDPR:

1. A breach of the transparency obligations under GDPR
2. Failure to establish a legitimate ground for handling the data

Transparency

Transparency is a core principle of GDPR. Principle (a) in GDPR Article 5 says that personal data shall be processed 'lawfully, fairly and in a transparent manner in relation to the data subject'. We've written before on the transparency obligation in data protection law for example when looking at the UK Emma's Diary decision last year - http://www.corderycompliance.com/ico-emmas-diary-data-disclosure-failure-case/.

CNIL said that information on Google's privacy practices was not easily accessible for users. It said that different parts of its practices were in different places and it said that sometimes up to 5 or 6 actions are required to get the information GDPR says Google should provide. CNIL was particularly critical of information on the use of geo-location in Android. It also said some information is not always clear or comprehensive.

CNIL also said that the purposes of processing were described in a too generic and vague a manner, as were the categories of data processed for these various purposes. It also said that Google had not made it clear enough which legal basis it relied on for processing data and how long it would retain data for.

Failure to establish a legitimate ground for handling the data

Google said that it relied on consent for the processing of data related to advertising. CNIL decided consent was not validly obtained since that consent was not sufficiently informed and that the consent was neither "specific" nor "unambiguous".

CNIL criticized the fact that some options were pre-ticked. It also said that since the user had to opt-in or opt-out of different types of processing in one bundle that consent did not satisfy the requirements of GDPR – CNIL said that "*GDPR provides that the consent is "specific" only if it is given distinctly for each purpose*."

What was the fine?

CNIL imposed a fine of €50m. Whilst significant this is less than the maximum of 4% of Google's worldwide revenue which would have led to a fine of about €3.9bn.

Are these the only complaints being handled by CNIL?

No. For our GDPR Navigator service (www.bit.ly/gdprnav) we keep a table of complaints by country. France is currently third in the table (behind the UK and Germany) having received 6,000 complaints by mid-November. In addition both LQDN and NOYB have brought additional complaints including a set of complaints about the subject access provisions of GDPR against Google subsidiary YouTube.

What are the takeaways?

It is wrong to say as some have done that this is the first GDPR fine. There have already been 59 GDPR cases in Austria for example. This case does however show that in appropriate cases DPAs will act fairly quickly and that they are prepared to hand out significant fines.

Lessons to be learnt from this case for GDPR include:

1. Transparency is a key GDPR obligation. Its been a key trend in enforcement action over the last year and this case shows that this trend is likely to continue. Consider reviewing your privacy policies and terms of use to ensure that they are intelligible, clear and transparent; also make sure that your data retention policies are in good shape.

2. Be clear on the basis you're relying on to process data. If that basis is consent or legitimate interests you'll need to clearly spell that out to data subjects. The fact you're talking to them on a small screen for a mobile app isn't an excuse.
3. The one-stop-shop won't apply in every case. Organisations need to have a clear regulatory strategy. They need to invest time to understand the strategy of the DPA they think will be their lead DPA but there are no guarantees that other EU DPAs won't investigate complaints too.
4. Privacy action groups will have success. These complaints were brought by two pressure groups who have previously taken action over data transfer. Both NOYB and LQDN have other complaints they are working on too.
5. GDPR has wide extra-territorial reach. We've had some conversations with people who feel that an EU regulator would not have the guts to take on a US corporation. This case shows that that's just wishful thinking. In appropriate cases DPAs will act regardless of the home country of the organisation concerned. Organisations will have to give proper thought to their internal structure as a result and particularly where decisions are made regarding data processing.
6. A privacy regulator can act fairly quickly and with relative ease – this case was brought in May, an online investigation was undertaken in September and a preliminary report (with a recommendation for a fine) was ready in October (the time taken after that was mainly to allow for a response to the findings, including an oral hearing).
7. Civil actions could result. Mr. Schrems has a long-running data protection collective action against Facebook which started before GDPR came in. A case like this with the changed regime under GDPR may help support a subsequent civil action. If that were the case, given then number of Android users across the EU, the claim could be significant even to an organisation of Google's means. We've talked previously about a similar civil action against Google in the UK in 2015 too - http://www.corderycompliance.com/data-protection-breaches-and-compensation-litigation-issues-for-consideration/

We report about data protection issues, including transparency under GDPR here: http://www.corderycompliance.com/category/data-protection-privacy/. Cordery's GDPR Navigator includes resources to help deal with data protection compliance – for more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong, Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH
Office: +44 (0)207 075 1784
Jonathan.armstrong@corderycompliance.com

André Bywater, Cordery, Lexis House, 30 Farringd Street, London, EC4A 4HH
Office: +44 (0)207 075 1785
Andre.bywater@corderycompliance.com