image: William Iven / Unsplash.com

José Lema Lawyer
jlema@ecija.com
Ecija, Madrid

Spanish Data Protection Authority fines Facebook €1.2 million for data protection infringements

The Spanish Data Protection Authority, following an investigation, has found that Facebook processes data, including sensitive data, for advertising purposes without obtaining adequate consent; it also found that Facebook does not delete users' data when requested to do so or where the data becomes no longer relevant. The Spanish Data Protection Authority's findings, and subsequent fine handed down to Facebook, represent the consequences of broader changes to how data processors are viewed within the EU.

Background

European data protection authorities have had Facebook in their sights for quite some time and not without reason: the American giant has been less than transparent in communicating how personal data is processed on its platform. However, only recently has the context shifted to one where the general public is much more conscious of data protection related issues, which has allowed the Spanish Data Protection Authority (hereinafter, 'AEPD') to confidently carry out an investigation in the context of a sanctioning procedure.

The AEPD took it upon itself to investigate Facebook's processing of personal data and whether it was compliant with the European regulations and the Spanish Data Protection Law (hereinafter, 'LOPD'). On the date the resolution was issued, the AEPD was able to use arguments backed by the CJEU and the Spanish Supreme Court to pin down Facebook Inc. to the local jurisdiction and apply the LOPD in full force. The investigation went on to find that Facebook Inc. was breaching several obligations of the LOPD, namely duly informing users about the data processing, duly obtaining users' consent for this processing, and duly removing data after being requested to do so or when data is no longer relevant.

Details of the proceeding

Facebook, Inc. as data controller

The AEPD did not accept Facebook's argument that the company that is bound by European data protection regulation is actually Facebook Ireland, Ltd, as accepted by European users when registering with the social network. The AEPD's counter argument was that, based on the Spanish Supreme Court's case law (STS 1384/2016), Facebook Inc. would be considered a data controller in any case:

"In its Opinion 1/2010, the Article 29 Working Party stated that 'The concept of controller is autonomous [...], and functional, [...] and thus based on a factual rather than a formal analysis.' [...] Google Inc., which manages the search engine Google Search, is a personal data controller, since it determines the ends, the conditions and the methods for the personal data processing."

Facebook Inc. is therefore identified as a data controller for users in the European Union, given its key role in the data processing.

Application of the LOPD

Following on from this premise, the AEPD analysed whether the LOPD is applicable to Facebook Inc., which would be the case for a data controller not established in Spain if a) the processing is carried out in the context of the activities of an establishment of the data controller, where the establishment is located in Spain, and b) where means located in Spain are being used in the processing of personal data. The AEPD quoted the CJEU judgment of 13 May 2014, reiterating that:

"[...] it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable."

Based on that reasoning, the AEPD found that Facebook Spain, S.L. could be considered an establishment located in Spain. The AEPD argued that the main purpose of Facebook Spain, S.L. is to attract advertisers to the platform, an activity that is causally linked with the data processing of Facebook Inc. This would guarantee the application of the LOPD to the facts at hand.

Furthermore, the AEPD also stated as a secondary argument that Facebook Inc. is using means located in Spain for the processing of personal data, namely the user's computers and the cookies therein installed. This alone would also be enough grounds for the LOPD to be applicable to the case at hand.

Information duty

The AEPD found that Facebook had infringed its duty to duly inform users regarding the collection and processing of data, the methods of processing and its purpose. The AEPD reached this conclusion after finding that:

- Facebook misguides users when obtaining consent, not disclosing that personal data other than that directly provided by the user will also be collected and processed. The use of multi-layered information makes it difficult for the user to grasp all relevant information.
- A 'data policy' is linked at the moment of registry, without making explicit reference to data protection. Accessing this policy is not mandatory prior to registration.
- Users are not provided with a list of the data that will be collected and processed.
- No options for guaranteeing parental consent for minors are enabled. Furthermore, advertising campaigns can target minors.
- Users are not warned that the cookies installed in their browsers can gather information even when they are not logged into the network.

Duty of obtaining consent

The AEPD found in its investigation that Facebook had infringed its duty to obtain free, unequivocal, specific and informed consent from its users. The AEPD reached this conclusion after finding that:

- The consent cannot be specific where the information is given by means of imprecise wording which does not allow users to understand how the data is processed and the purpose of the processing.
- The data collected is not proportional in connection with the purpose of the processing, much less where the user is giving misinformed consent.
- The word 'finished,' instead of 'I accept,' is used when completing user registration. Furthermore, users are not required to have consulted the data privacy policy prior to consenting.
- Considering that the information shown by Facebook can confuse the average user of new technologies, the consent can never be unequivocal or specific.

Sensitive personal data

Some duties are stricter when referring to the sensitive personal data of Facebook users:

- Facebook collects and processes sensitive personal data, which it uses to build profiles, even after informing the user that his/her sensitive personal data will not be used for advertising.
- The tools provided to advertisers allow them to target the public based on sensitive data such as sexual life, beliefs or health.
- For sensitive data, the consent must be explicit and in writing, and Facebook does not comply with these requirements.

The duty to remove data

The AEPD found that Facebook had infringed its duty to remove personal data where it is no longer necessary for the purpose for which it was collected. The AEPD reached this conclusion after finding that:

- Where a user configures their privacy settings so that ads are not served based on personal data, the profiling data collected by Facebook is not erased but stored.
- The IP addresses from where connections have been established are stored for at least 11 months, which could lead to the identification of the physical location of a user.
- After deletion of an account, a cookie associated with the cancelled profile could be associated to a new user registered with the same email for up to 17 months.

Sanctions

The AEPD imposed the following fines:

- For breaching Article 6.1 of the LOPD, constituting a serious infringement: €300,000.
- For breaching Article 7 of the LOPD, constituting a very serious infringement: €600,000.
- For breaching Article 4.5 of the LOPD, constituting a serious infringement: €300,000.

The AEPD handed down the largest sanction available for each of the infringements, taking into account aggravating facts such as the infringement being continued, the volume of the processing carried out, the link between Facebook's activity and the personal data processing, Facebook's turnover created as a direct result of the infringements and Facebook's intentionality in its conduct.

What the decision tells us about large-scale data processing

The decision itself does not mark a sudden change of direction in the manner in which data processors are regarded in Europe. Rather, the AEPD resolution is but a consequence of a much broader and slower process, of which the ultimate result is the EU General Data Protection Regulation (the 'GDPR').

This Regulation is what should be taken into account by large scale data processors in their handling of personal data. Data controllers that process personal data of European individuals have been sufficiently warned and given enough time to accommodate the requirements of the GDPR. This fine is but a reminder that local data protection agencies will start taking measures if they believe that the provisions of the GDPR or the local regulations are not being complied with.

Arguments for pinning down international operators to not only the European, but also local jurisdiction, are now fully backed by the CJEU and even local Supreme Courts. This current doctrine is much more in line with what the GDPR has in store: Article 2 states that the GDPR shall apply to controllers not established in the EU where the processing of personal data of European data subjects is related to (a) the offering of goods or services; or (b) the monitoring of their behaviour.

It is clear that the activity of many international operators, including Facebook, falls within those definitions, and therefore they will have to comply with the dispositions of the European Regulation when it enters into force. Finally, this decision corroborates that businesses, European and non-European, will have a harder time complying with European data protection regulations, which will result in a double-edged effect.

On the one hand, non-EU companies will be more dubious about offering their services in Europe, where those services imply the processing of personal data - which might be especially harmful, considering the universality of internet-borne, information technology services. On the other hand, European companies, especially newly formed companies, will have to bear a heavy compliance burden that simply will not exist for non-EU competitors.

All of this could result in innovation stagnation for European companies, which may become incapable of competing in an environment based on novelty and speed.