Cybersecurity, Data Privacy & Information Management Alert

Weil

August, 2019

Enforcement under the GDPR – the new paradigm

By Barry Fishley and Muzaffar Shah

Barry Fishley
View Bio
barry.fishley@weil.com
+44 20 7903 1410

Muzaffar Shah
View Bio
muzaffar.shah@weil.com
+44 20 7903 1090

The GDPR marked its first anniversary on Saturday, 25 May 2019. Before the GDPR came into effect, organisations were understandably apprehensive about the exponential increase in potential fines under the new regime. During 2018, the level of fines seen did not represent a significant increase on pre-GDPR fines for breach of data protection laws. However, the landscape has now significantly changed with a number of multi-million pound fines demonstrating regulators' willingness to use their new enforcement powers.

The Google Fine

The innocuous-looking Article 12 of the GDPR on the transparency of language formed much of the basis for the first large fine issued by a supervisory authority. On 21 January 2019, the French National Data Protection Commission (the "**CNIL**") imposed a fine of **€50m** on Google LLC for lack of transparency, inadequate presentation of fair processing information and the lack of valid consent to the personalisation of advertisements. The CNIL's investigation into Google originated from complaints brought by two privacy advocacy groups.

The CNIL detailed various contraventions but in particular raised the following issues:

- a lack of accessibility of information, citing that data subjects need to undertake five actions in order to find information about data processing relevant to the personalisation of advertisements;
- inadequate information about data retention periods;
- vague and broad descriptions of the purposes for data usage; and
- consent gathering mechanisms which failed to meet the requirements of the GDPR for specific and unambiguous consent.

The level of the CNIL's fine was influenced by the "massive and intrusive" nature of Google's data processing as well as the "key" nature of the GDPR provisions which were contravened.

The CNIL's comments on privacy notices will be of interest to all organisations, particularly in respect of Article 12, where, far from representing aspirational standards in respect of the clarity of language, the CNIL used the GDPR's transparency requirements as a basis for levying this substantial fine. What is clear is that, particularly for technology companies providing complex online services, there is a very difficult balancing act to achieve between providing sufficient information

to meet the information requirements of the GDPR and not providing excessive or disparate information in a manner which contravenes the principle of transparency.

Unsurprisingly, Google has appealed the CNIL's fine and proceedings before France's Supreme Administrative Court remain underway.

Takeaways

It is clear that the following is recommended:

- Have fair processing information in one document.
- Specify which processing is based on consent and which processing is based on legitimate interests.
- Do not use pre-ticked boxes.
- Obtain consent for each specific purpose that requires consent instead of obtaining consent for all purposes together.

One Stop Shop

Under the 'one-stop shop' principle, an organisation that carries out cross-border processing of personal data in multiple Member States generally only has to deal with the regulator in the location of its main establishment. Even though Google's European headquarters is in Ireland, the 'one-stop shop' principle was determined not to apply.

CNIL held that Google did not have a 'main establishment' in Europe because the decision making in relation to the processing of personal data was carried out in the U.S..

Accordingly, in theory Google could face enforcement action from other European data protection regulators.

How Can Organisations structure themselves to Use the 'One-Stop Shop'?

- Ensure that an establishment in the EEA has effective power to make decisions on the processing of personal data.
- List the European establishment in the privacy policy as a contact address and/or as the controller of personal data.
- Consider having the European establishment appoint a data protection officer.

The British Airways Fine

On 8 July 2019, the UK supervisory authority, the Information Commissioner's Office (the "**ICO**"), issued a notice of intention to fine British Airways **£183.39m** for contraventions of the GDPR as a result of a cyber-incident notified to the ICO in September 2018.

At this stage, the ICO has not provided detailed reasons for the staggeringly high level of the fine beyond a brief statement referring to the following factors:

- the number of records compromised (500,000);
- the types of data involved – log in data, payment card information, travel booking details and names and addresses; and
- the nature of the breach – the redirection of customers to a "fraudulent site".

The level of the fine represents 1.5% of BA's worldwide turnover in 2017. Therefore, although the fine is less than the maximum fine of 4% of worldwide turnover, it is still by far the largest fine proposed by a European supervisory authority to date.

BA has stated that it is "surprised and disappointed" by the ICO's decision, pointing out that the breach stemmed from third party criminal conduct with no evidence of fraudulent activity being conducted on the accounts linked to the theft. However, we can conclude that the ICO must have considered that the security measures which BA had adopted to protect its website were not "adequate" for the purposes of the GDPR.

The ICO's investigation was conducted under the "one-stop-shop" principle since there are citizens of other EU Member States whose data was involved in the breach. BA and other European regulators have 28 days from 8 July 2019 to make representations concerning the fine. BA has already signalled its intention to challenge the level of the fine, but accepts that a contravention of the GDPR occurred.

The Marriott Fine

On 9 July 2019, the ICO issued a notice of intention to fine Marriott International ("**Marriott**") £99,200,396 for infringements of the GDPR. The proposed Marriott fine relates to a cyber-incident, which was notified to the ICO by Marriott in November 2018. A variety of personal data contained in approximately 399 million guest records globally was exposed by the incident, of which around 30 million related to residents of 31 countries in the European Economic Area ("**EEA**"). The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought the Starwood hotels group in 2016, because the vulnerability originated from insecure systems within the Starwood group, which were compromised in 2014. The exposure of customer information was not discovered until 2018. The ICO said that organisations must be accountable for the personal data they hold which "include carrying out proper due diligence when making a corporate acquisition, and putting in place proper accountability measures to assess not only what personal data has been acquired, but how it is protected."

The ICO had been investigating this case as lead supervisory authority on behalf of other EU Member States, under the GDPR 'one stop shop' provisions, as mentioned above.

Take Away

It is noteworthy that BA and Marriott are not technology companies undertaking complex operations with personal data – the type of organisation that many have considered are most vulnerable to large data protection fines. Large and small organisations will be following the ICO's actions with great interest.

The view elsewhere

The first year under the GDPR saw a total of 446 cross-border cases being logged in the European Data Protection Board's case register. 205 of these cases resulted in one-stop-shop procedures under the GDPR with 19 final outcomes under the one-stop-shop procedure. This activity has evidenced a very large degree of cooperation between data protection authorities.

The ICO has posted 46 decisions since the GDPR came into effect. Other than the prospective BA and Marriott fines detailed above, the largest fine under the GDPR issued in this period was a fine of £365,000 issued to Uber for failing to protect customers' personal information during a cyber-attack.

Most national European regulators reported an increase in the number of queries and complaints received in 2018 compared to 2017. The total number of inquiries and complaints in the period was over 144,000, whilst 89,000 data breach notifications were received. The ICO has noted that approximately 50% of the complaints that it received relate to data subject access requests.

The European Data Protection Board has stated that the increased number of questions and complaints referred to regulators confirms a perceived increase in awareness of data protection issues among individuals. For controllers and consumer facing businesses in particular, this should equate to greater vigilance, since more complaints means a greater risk of contraventions being recognised and being referred to a regulator.

Although fines other than the BA, Marriott and Google fine have tended to be in the hundreds of thousands of Euros at most, there are a number of ongoing investigations which may result in further large fines. Last month, the Irish Data Protection Commissioner began a statutory inquiry into Google's personalised online advertising.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Cybersecurity, Data Privacy & Information Management Group.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Muzaffar Shah	View Bio	muzaffar.shah@weil.com	+44 20 7903 1090