RECORD GDPR FINES AND WILL GDPR CLASS ACTIONS BE MORE DIFFICULT IN THE UK?

DECEMBER 2021

By Barry Fishley, Hannah Rumble and Victoria Dyer

Record EU GDPR fine for Amazon

Amazon has received a €746 million (£636 million) fine for allegedly breaching the EU General Data Protection Regulation ("**EU GDPR**"). It is the largest fine issued to date for breaches of the EU GDPR since it took effect in May 2018. The fine was issued by Luxembourg's data protection authority, the National Commission for Data Protection (the "**CNPD**"), as the result of a complaint filed in 2018 by the French privacy rights group La Quadrature du Net. The fine was only made public as a result of it being disclosed in Amazon's quarterly regulatory filing in the US on 30 July 2021.

The specifics of the conduct that gave rise to the fine is not public. La Quadrature du Net's complaint was filed on behalf of 10,000 people, claiming that Amazon's advertising targeting system was carried out without 'free consent' in violation of the EU GDPR, but the CNPD's professional secrecy obligations under local Luxembourg laws prevent the release of the CNPD's decision at this stage. Amazon stated that "*there has been no data breach, and no customer data has been exposed to any third party… the decision relating to how we show customers relevant advertising relies on subjective and untested interpretations of European privacy law, and the proposed fine is entirely out of proportion with even that interpretation*". We can speculate that the fine therefore relates to targeted advertising.

Amazon filed an appeal to the decision made by the CNPD at the Luxembourg Administrative Tribunal on 15 October 2021. The organisation refused to comment on the appeal.

ICO confirms intention to fine Clearview AI Inc over £17 million for alleged serious breaches of UK data protection laws

The ICO has announced it has issued a notice of intent to impose a fine of £17 million on Clearview AI Inc ("**Clearview**") and a preliminary enforcement notice requiring the company to cease further processing of the personal data of data subjects in the UK and delete the data it holds, due to alleged serious breaches of the UK GDPR and the Data Protection Act 2018.

This action was taken in response to the findings of a joint investigation conducted by the ICO and the Office of the Australian Information Commissioner ("**OAIC**") into Clearview's data processing practices. The ICO's preliminary view is that Clearview's use of images, data scraped from the internet and biometrics for facial recognition involved the processing of personal data of a substantial number of people from the UK and may have breached UK data protection laws in several significant respects. These include Clearview''s alleged failures to: provide data subjects in the UK with fair processing information about what is happening to their data; comply with the enhanced data protection standards under the UK GDPR for processing special category data; process data fairly, lawfully, and transparently in accordance with the first data protection principle and have a lawful basis established to collect the data, under the UK GDPR; and prevent the data from being retained indefinitely, in breach of Article 5(1)(e), UK GDPR.

Although the ICO acknowledged Clearview's facial networking service is no longer available in the UK, it believes it has cause to suspect that the company may still be processing significant volumes of UK citizens' information without their knowledge, and determined accordingly that preliminary enforcement action was necessary. Clearview has the right to submit representations concerning the allegations raised by the ICO. A final decision from the ICO is not anticipated until mid-2022.

Twitter fined €450,000 by Irish DPC

Twitter has received a fine of €450,000 for failure to give proper notice of a data protection breach within the required timeframe under EU GDPR and for providing a lack of sufficient detail in relation to the breach. Subsequently, the Data Protection Commission (the "**DPC**") found Twitter to be in breach of Article 33(1) and 35(5) of the EU GDPR.

The breach related to a bug in Twitter group's Android app and was discovered on 26 December 2018 by an external contractor managing Twitter Inc.'s "bug bounty programme". As a consequence of the bug, if a user operating an Android device changed the email address associated with that user's Twitter account, the user's tweets became unprotected and accessible to the wider public without the user's knowledge. It was identified that at least 88,726 EU and European Economic Area users were affected between 5 September 2017 and 11 January 2019. Twitter Ireland confirmed that the bug appeared from 4 November 2014, but that it could not identify users affected prior to 5 September 2017, meaning more users may have been affected, over and beyond the number disclosed.

RECORD GDPR FINES AND WILL GDPR CLASS ACTIONS BE MORE DIFFICULT IN THE UK?

DECEMBER 2021

According to Twitter Ireland – the data controller – the breach had arisen in the context of processing carried out on its behalf by Twitter Inc. – the data processor. The issue was reported to Twitter Inc. on 29 December 2018. Twitter Inc. subsequently assessed the issue as potentially being a personal data breach on 3 January 2019 and triggered the company's incident response process on 4 January 2019. However, the Twitter Group's DPO and Twitter Ireland were not notified until 7 January 2019. The data breach was reported to the DPC on 8 January 2019.

The DPC found that it is the controller's responsibility to ensure that it becomes aware of a breach in a timely manner so that it can comply with its obligations under Article 33(1) of the EU GDPR. In assessing this, the DPC also considered Article 5(2), which gives the controller overarching responsibility for ensuring compliance with the EU GDPR. The DPC also found that Twitter Ireland failed to comply with its obligations under Article 33(5) of the EU GDPR in that the information furnished by it did not contain sufficient detail so as to enable the question of its compliance with the requirements of Article 33 of the EU GDPR to be verified. Twitter Ireland had produced an "Incident Report" which it submitted was the primary record in which it documented the facts, effects, and remedial action taken in respect of the breach. However, the DPC found that the Incident Report was insufficient on the basis that it failed to contain all material facts relating to the notification of the breach. Specifically, the report did not contain any reference to, or explanation of, the issues that led to the delay in Twitter Ireland receiving notification and did not address how Twitter Ireland assessed the risk arising from the breach to affected users.

Ultimately, the delay in notifying the DPC of the data breach and the number of data subjects who were affected by the breach were arguably the DPC's most decisive factors in making its final decision.

Take Aways

- The fine against Amazon indicates that supervisory authorities are now prepared to fully exercise their rights under the GDPR with respect to the level of fines and therefore heightened the risk profile for non-compliance particularly where there are large volumes of data subjects concerned.
- The Twitter fine highlights the need for organisations to standardise and train staff on the reporting of personal data breaches. Organisations should consider standardising reporting processes so as to make certain that, in the event of a data breach, the necessary reports are appropriately formatted and sufficiently detailed. It is also an important reminder that in any acquisition of a business, the due diligence process should involve checking that the target has a data breach incident response plan in place which, among other things, recognises the time lines required with respect to notification of a data breach (being in some cases no later than 72 hours).

Supreme Court rejects right to bring representative class action under DPA 1998

On 10 November 2021, the UK Supreme Court handed down its decision in *Lloyd v Google LLC*. The claimant brought representative (opt-out) action against Google LLC and sought damages under section 13 of the Data Protection Act 1998 ("**DPA 1998**") for a uniform per capita sum on behalf of more than 4 million Apple iPhone users resident in England and Wales. The claimant alleged that Google had unlawfully tracked the users' internet activity without their consent in breach of data protection laws.

The Supreme Court concluded that s13(1) of the DPA 1998 cannot reasonably be interpreted as conferring a right to compensation for a breach without evidence of "material damage" in the form of financial loss or mental distress – "loss of control" of personal data would not be enough to amount to material damage under the DPA 1998. In any case, had the claim been for financial loss or mental distress, the class action would have been unfeasible. The individual effect of the breach would differ from person to person, with each individual experiencing different levels of financial loss or mental distress, subsequently defeating the "same interest" requirement for class actions.

RECORD GDPR FINES AND WILL GDPR CLASS ACTIONS BE MORE DIFFICULT IN THE UK?

DECEMBER 2021

The Court suggested that it may be appropriate for future claimants with similar claims to bring bifurcated proceedings. Such proceedings would require claimants to first bring a representative action to establish the defendant's liability, followed by an individual claim for compensation. Therefore, although similar representative claims can theoretically be brought in future, the legal and practical challenges of economically doing so, as recognised by the court, mean similar claims may be less appealing to prospective claimants and litigation funders who would not see the reward in paying for litigation solely to determine liability and not damages.

Take Away

Importantly, the decision was made under the now-repealed DPA 1998. The Court declined to be drawn into discussing the GDPR, leaving the position for similar claims under the current regime unclear. There are potentially material differences in the statutory regimes, especially given that Recital 85 of the GDPR provides that "a personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data ..." which suggests that, with regard to data breaches, a mere loss of control of personal data may amount to damage and the right to compensation under Article 82 of the GDPR without the need to prove either financial loss or distress. In the meantime and helpfully for organisations, the decision in *Lloyd v Google LLC* will likely curb some of the momentum that had been building around potential scope for class action opt-out claims in data breach cases.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any of the authors listed below.

Barry Fishley	View Bio	barry.fishley@weil.com	+44 20 7903 1410
Hannah Rumble	View Bio	hannah.rumble@weil.com	+44 20 7903 1491
Victoria Dyer		victoria.dyer@weil.com	+44 20 7903 1610

© 2021 Weil, Gotshal & Manges (London) LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges (London) LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to subscriptions@weil.com.