May 2019

GDPR One Year On - The Regulators are Coming

Saturday 25 May marked the first anniversary of the new era heralded by the General Data Protection Regulation ("**GDPR**"). This milestone serves as a timely opportunity to consider a number of recent decisions from various national regulatory authorities. These enforcement actions have underlined the importance of companies ensuring that they gather and process personal data in compliance with data protection law, including GDPR. While decisions of other national regulatory authorities are not binding in Ireland, they will be instructive given that they are based on the same underlying principles, which are derived from GDPR.

Polish company fined for unlawful processing of publicly-available data

Poland's Personal Data Protection Office (the "**UODO**") announced a fine of approximately €220,000 in March against an unnamed company that processed contact data obtained from publicly available sources without informing the individuals concerned. Article 14 of GDPR requires data controllers who do not obtain personal data directly from the data subject to provide these individuals with information about how their data is processed within a reasonable time after obtaining the data, but this is not required where it "proves impossible or involves a disproportionate effort".

The company obtained personal data from public registries, such as the Polish electoral register, to prepare trade reports, contact lists and "other business and management consulting services" to its clients. It sent the requisite data processing statement to the data subjects whose email addresses it had and published a similar data protection policy on its website. However, the company did not provide this information to the over 6,000,000 data subjects for

For further information on any of the issues discussed in this article please contact:

Lorcan Tiernan
DD: + 353 (0)1 673 1736
lorcan.tiernan@dilloneustace.ie

Joseph Lynch
DD: + 353 (0)1 673 1890
Joseph.lynch@dilloneustace.ie

whom it did not have email addresses but did have phone numbers or postal addresses.

The UODO decided that the provision of the information through a website privacy policy did not suffice as it was neither impossible nor a "disproportionate effort" for the company to contact the individuals whose telephone number or postal address were available, despite the company's argument that the cost of doing so would have been excessive. The UODO agreed that, where the company did not possess any contact details for the data subjects, it would not be obliged to find these contact details as this would involve a "disproportionate effort".

The UODO noted that it decided to impose a fine as the company in question was aware of its obligations under Article 14 of GDPR, and decided not to inform data subjects of the manner in which their personal data is being processed in order to avoid the costs of doing so. The company was also ordered to belatedly provide the requisite information to the data subjects whose contact data it held on file. This decision serves as an instructive reminder of the fact that personal data might be publicly available does not necessarily mean that that data may be processed. The principles set out in GDPR and the relevant national legislation in relation to having a legal basis for data processing still apply.

UK Company fined for selling personal medical data

The United Kingdom's Information Commissioner's Office (the "ICO") fined Bounty (UK) Limited £400,000 in April for illegally sharing personal data belonging to more than 14 million data subjects.

This company operated a pregnancy and parenting club, and as part of its operations it collected personal data for the purpose of registering members through its website and mobile app, merchandise pack claim forms or directly from new mothers at hospital bedsides. However it also supplied approximately 34.4 million records between June 2017 and 30 April 2018 to credit reference and marketing agencies for the purposes of electronic direct marketing. The personal data shared included health data such as the pregnancy status of new mothers and mothers-to-be (which is a special category of personal data subject to additional protections under GDPR), as well as the birth date and gender of newly-born children.

While the ICO found that the online registration methods included privacy notices which included "a reasonably clear description of the organisations they might share information with", none of the merchandise pack claim cards or offline registration methods contained an option to opt in to direct marketing.

As the breaches occurred before GDPR came into force, the company was fined £400,000 under the UK's pre-existing data protection rules (under which the maximum possible fine was £500,000). The ICO also noted that the breaches were motivated by financial gain as the data sharing was "an integral part of their business model at the time" and that they were "unprecedented" in scale. This, along with the fact that personal health data and the personal data of children were involved, may be considered to have influenced the ICO in imposing a fine which was at the upper end of the scale that applied at the time. A much higher fine may have been imposed if the breaches had occurred after GDPR came into force, as the maximum possible fine is now €20,000,000 or 4% of a company's annual global turnover.

This case underlines the serious nature of companies' obligations in relation to collection, processing and sharing of personal data.

Facebook ordered not to bundle data collected from different services in Germany

Germany's competition enforcement authority, the Bundeskartellamt, announced in February that it had found that Facebook's data protection practices were in violation of German competition law. In brief, the Bundeskartellamt found that (i) Facebook occupied a dominant position in the German market for social networks; and (ii) Facebook's practice of combining user data gathered from different services (such as Facebook itself, Instagram and Whatsapp) as a condition of using these services constituted an abuse of its dominant position. The Bundeskartellamt has ordered Facebook to offer its services to its German customers without bundling user data gathered from these different services.

While the Bundeskartellamt's decision was based on competition law, it did also express the opinion that there was no legal basis under GDPR which allowed Facebook to process the data collected in this manner. It ordered Facebook to only bundle user data gathered from different services in the case of users who have been allowed a real choice in the matter.

As this decision was based on German domestic competition law, it remains to be seen whether the same approach will be taken by the other national competition enforcement authorities or the European Commission. However at the very least it will give businesses reason to consider whether their data processing practices or trading terms could be construed as abusive. It also demonstrates that data protection cannot be properly assessed in isolation from other aspects of legal compliance. The intersection between competition law and data protection law in particular looks set to become a focus of attention from the domestic regulators in the coming years, and it is noteworthy that Ireland's Data Protection Commission has been active in scrutinising Facebook's proposed integration of those services in Ireland.

Conclusion

GDPR has now been in force for one year, and regulatory investigations are proceeding in earnest. In Ireland, the Data Protection Commission has already announced investigations into personalised online advertising and the sufficiency of technical and organisation measures taken by IT companies such as Twitter and Facebook to protect the security of personal data. This suggests that tech companies will face particular supervision by the Data Protection Commission, but it remains as important as ever for all businesses to ensure that their data protection procedures are beyond reproach.

Should you have any queries in relation to the issues raise in this bulletin, please contact the authors or your usual Dillon Eustace contact for further information.

Dillon Eustace
May, 2019

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.