Enforcing the GDPR — what lies ahead?

Mark Rasdale, Partner, and Davinia Brennan, Associate, at A&L Goodbody consider what regulatory action we can expect to see in the coming months and years and the practicalities of enforcement

The first five months of the General Data Protection Regulation ('GDPR') have been busy for EU Supervisory Authorities ('SAs'). At the time of writing, over 80,000 breach notifications have reportedly been received by SAs. The Irish Data Protection Commission ('DPC') has yet to issue any fines or other sanctions, but organisations should not become complacent, as enforcement action is inevitably on the horizon. The DPC has warned us that whilst it intends to continue an engaged supervisory approach, it will also be imposing fines and other sanctions as necessary and proportionate.

Post-GDPR regulatory activity

Since 25th May 2018, the DPC has received 1,700 complaints and 2,500 breach notifications, which represents a doubling of complaints and almost three times the number of breach notifications on the same period in 2017. The majority of complaints continue to concern data access requests, in particular the non-disclosure of full data. Disclosure of data without a legal basis is also a frequent complaint. Many of the complaints concern the financial services sector and technology companies, likely due to the large amount of personal data processed by them.

It is clear that SAs are concerned about being inundated with breach notifications. The DPC has publicly stated that both under and over-reporting data breaches could attract enforcement action. Therefore accountability, and being able to justify why you are notifying, or have decided not to do so, is key. With this upward trajectory in the volume of complaints and breach notifications, it is not surprising that the DPC has received an increased regulatory budget for the coming year, totalling €15.2 million.

Regulatory trends — focus areas

The DPC will continue to have a leading profile when it comes to international enforcement. In October 2018, the DPC confirmed that it had launched an investigation under section 110 of the Data Protection Act 2018 ('2018 Act') into a Facebook security breach which gave hackers unauthorised access to approximately 30 million users' accounts. In particular, the investigation will examine Facebook's compliance with its obligation under the GDPR to implement technical and organisational measures to ensure the security and safeguarding of the personal data it processes.

Whilst the DPC's investigative and enforcement activities will be primarily directed by complaints and breach notifications, it will also have power to commence investigations at its own initiation in order to tackle suspected infringements of the GDPR or 2018 Act.

It is likely that we will see a more sectoral approach to enforcement. Just three days after the GDPR took effect, the DPC published a Special Investigations Report into Privacy in the Hospitals Sector, which identified 35 risks and 76 recommendations to mitigate those risks. The purpose of the investigation was to bring to the attention of every hospital in the State, the matters of concern the DPC found in the sample of twenty hospitals inspected.

In the post-GDPR environment, the DPC has confirmed it will be proactively targeting its enforcement activities at sectors involved in large-scale data processing activities that constitute a high risk, such as online tracking, automated decision-making and profiling; processing of high-risk data, such as health, biometric, financial or insurance data; and processing using emerging technologies.

Regulatory priorities — transparency will be key

The DPC has stated that assessing compliance with the transparency requirements under the GDPR and privacy notices will be a priority focus area in the short term. This assessment can be done in a relatively hands-off manner, particularly where it involves an assessment of compliance with the requirements under Article 12, 13 and 14 of the GDPR, and the related Guidelines on Transparency (WP260), produced by the previous Article 29 Working Party and endorsed by the European Data Protection Board. Not unlike breach notifications

and data access requests, the privacy notice — the public statement of what organisations are doing with personal data — could well become a trigger for deeper regulatory investigations. The DPC has also emphasised that it is imperative, in line with the principle of accountability in the GDPR, that organisations can stand over and justify their data processing arrangements and be able to demonstrate compliance.

Personal criminal liability

Personal liability for data protection offences is likely to come to the fore in the new data protection landscape. The 2018 Act enables the DPC and Director of Public Prosecutions, respectively, to prosecute controllers and processors for summary and indictable offences.

There are nine criminal offences under the 2018 Act. Section 146 provides that where an offence is committed by a body corporate and is done with the consent or connivance, or could be attributable to the neglect of a person, that person, as well as the body corporate shall be guilty of an offence. A person can be a director, manager, secretary or other Officer of a company purporting to act in that capacity. Hence, data risk has become a mainstream corporate boardroom concern. Senior management cannot afford not to be pro-actively involved in data risk management issues.

Data protection litigation on the rise

We can expect to see a notable increase in the volume of data protection litigation. Section 117 of the 2018 Act provides for the possibility of a data protection action being brought against a controller or processor. Such actions will be founded in tort. While this is not new, a data subject now has an express right to be compensated for non-material damage (i.e. emotional distress) as a result of data protection breaches, so the nature of actions and the type of losses claimed will change significantly.

> ***"Not unlike breach notifications and data access requests, the privacy notice — the public statement of what organisations are doing with personal data — could well become a trigger for deeper regulatory investigations."***

The 2018 Act (in sections 117(7) and (8)) also allows a data subject to mandate a not-for-profit organisation to take a representative action on his/her behalf seeking an injunction, declaration, or compensation for data protection breaches. It remains to be seen how this provision will be used in practice, particularly in relation to the challenges in managing, funding and proving loss in such actions.

For more on the changed litigation landscape, see the article on pages 7-8 of this edition.

Class actions

While it was initiated pre-GDPR, a decision given in the UK is informative of the issues that may arise if similar actions are brought in Ireland. *Lloyd v Google* [2018] EWHC 2599 (QB) concerned the so-called 'Safari Workaround', by which Google allegedly collected individuals' web browsing data in 2011-2012, bypassing privacy settings on iPhone browser software.

The main issues raised by the application were whether the pleaded facts disclosed any basis for claiming compensation under the UK Data Protection Act 1998, and if so, whether the Court should permit the claim to continue as a representative action.

The Court dismissed Mr Lloyd's representative action, finding firstly that he had not proved any material or non-material loss had resulted from the breach, and secondly, that the class of claimants was so large that members of the class did not have the 'same interest' (a UK procedural requirement in order to be permitted to proceed with a representative action). So while there is understandable concern about the prospect of 'class actions' in the new data landscape, and the litigation risk is certainly greater now than before, this case serves as an important reminder that not all claims brought in these circumstances will be viable and without challenge.

Vicarious liability

Employers are also likely to see an increase in vicarious liability actions for data protection breaches committed by employees as a result of a recent landmark ruling by the UK Court of Appeal in *Wm Morrisons Supermarkets Plc v Various Claimants* [2018] EWCA Civ 2339. Morrisons was held vicariously liable for an employee's deliberate disclosure of co-workers' personal data on the internet, even though the breach was targeted at harming Morrisons. The amount of damages that Morrisons will have to pay to the 5,518 employees who took the case has yet to be determined. The Court acknowledged that data breaches caused by individuals acting in the course of their employment may lead to a large number of claims against companies for 'potentially ruinous amounts', but that the solution is to insure against such catastrophes. The decision could be of persuasive authority to the Irish courts.

Secondary liability

Article 82 of the GDPR allows a data subject to claim full compensation for damage resulting from a data breach from either a controller or processor. The controller or processor can then claim back from the other the propor-

(Continued on page 6)

(Continued from page 5)

tion of the compensation corresponding to its part of the responsibility for the damage. As a result, negotiations regarding data risk and liability issues are becoming more involved. Where controllers and processors both have an obligation to ensure appropriate security, it seems just a matter of time before we begin to see some secondary litigation between them, particularly in the context of personal data breaches.

Practicalities of enforcement

Part 6 of the 2018 Act grants the DPC greater discretion in regards to handling complaints and conducting investigations into suspected infringements of data protection law.

Amicable resolution

For all complaints, the DPC will first assess whether an amicable resolution may be reached between the complainant and controller or processor. Where the DPC determines there is a reasonable likelihood of the parties reaching an amicable resolution within a reasonable time, the DPC may attempt to facilitate such a resolution. This in effect involves the DPC acting as a mediator in the dispute.

Summary examination

If the DPC elects not to follow the amicable resolution procedure or it does not succeed in achieving a resolution, then it will take one or more of the following actions:

- reject the complaint;
- dismiss the complaint;
- provide advice to the data subject in relation to the complaint;
- serve an enforcement notice requiring the controller or processor to take specified action;
- conduct a formal inquiry into the complaint; or
- take such other action as it considers appropriate

Formal inquiry under Chapter 4 and/or 5

If the DPC decides to conduct a formal inquiry into a suspected infringement as a result of a complaint or of its own volition, it has the option of: (i) causing an investigation to be carried out using its Chapter 4 investigation powers; and/or (ii) causing a full investigation under Chapter 5 to be carried out.

Under Chapter 4, the DPC, through an authorised officer ('AO'), has extensive powers to enter business premises unannounced and without a court ordered search warrant. Warrants are only required in regard to private dwellings or where an AO is prevented access to business premises. AOs may search and inspect, demand and take copies of records relating to the processing of personal data. Anyone who obstructs such an inquiry could be guilty of an offence. Information or enforcement notices may also be served requiring a controller or processor to provide certain information, or take specified steps. It is an offence to fail to comply with these notices. Where there is a need to act urgently to protect data subjects, the DPC may apply to the High Court for an order suspending, restricting or prohibiting data processing operations, for such period as specified in the order. It is possible for the DPC to switch from a Chapter 4 to a Chapter 5 investigation at any time.

A Chapter 5 investigation is a quasi-judicial inquiry by the DPC. The DPC may appoint an AO to undertake the investigation and to prepare an investigation report. For the purposes of the investigation, the AO may order the production of documents, require a person to answer any questions under oath, and may conduct a private oral hearing. It will be an offence for a controller or processor to withhold, destroy or refuse to provide any information or to obstruct an AO. The AO's draft report will be subject to submissions by the party being investigated, before being submitted to the DPC. The investigation report shall state whether the AO is satisfied or not that an infringement has occurred and why. However, the AO is not empowered to make any recommendation in regard to any sanction that ought to be imposed by the DPC. That is a matter entirely reserved for the DPC. The final report will be considered by the DPC, following which the DPC may invite further submissions, or conduct an oral hearing. The DPC must then reach a final decision as to whether an infringement has occurred, and if so, whether to impose a fine or other corrective power. Any such decision may be appealed to the Circuit or High Court. If there is no appeal, any administrative fine imposed must be confirmed by way of application to the Circuit Court.

Conclusion

More than ever before, personal data requires careful management and continual investment. Personal data are now no different to any other valuable corporate asset, and companies need to be able to react quickly and effectively when the integrity of that asset is put at risk.

The DPC has emphasised the importance of a pro-active, engaged supervision approach to how it regulates. For organisations in this new data landscape, an engaged and pro-active approach to compliance is equally important. The compliance burden is high, and so too is the potential impact if that burden is not met.

Mark Rasdale and Davinia Brennan
A&L Goodbody
mrasdale@algoodbody.com
dbrennan@algoodbody.com