LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

DPC publishes first Annual Report since GDPR

by **lk-shields**

DPC publishes first Annual Report since GDPR

5th March 2019 | by

The EU-wide implementation of the GDPR on 25 May 2018 also marked the commencement in Ireland of the Data Protection Act 2018 and the establishment of a new Data Protection Commission. The DPC's first annual report was published on 28 February 2019, covering the period 25 May to 31 December 2018.

Whilst the GDPR is the main focus of the annual report, it also deals with the DPC's supervisory role under the Law Enforcement Directive (2016/680), which was transposed into Irish law by the 2018 Act, and the e-Privacy Regulations (S.I. No. 336 of 2011), in respect of the processing of personal data in the context of electronic communications.

Increased activity

The DPC has been busy post-GDPR, receiving nearly 31,000 communications during the report period. This was anticipated, and the DPC significantly tooled-up well before May 2018. Its resource allocation in 2016, when the GDPR was first adopted, was broadly €4.7 million funding and 52 staff, compared to €15.2 million funding for 2019 and a current headcount of 135, with further recruitment planned in 2019.

Complaints profile

2,864 complaints were received by the DPC during the report period. Consistent with previous years, complaints regarding 'access requests' make up the largest compliant type. Complaints relating to unfair processing and disclosure were also high, followed by complaints made under the ePrivacy Regulations in respect of various forms of electronic direct marketing.

32 new complaints were investigated under the ePrivacy Regulations, some of which concluded with District Court prosecutions. This will become a key area for complaints and enforcement once the long awaited EU-wide ePrivacy Regulation is finalised and becomes enforceable.

The DPC's newly formed LED Complaints Unit handled seven complaints in relation to the Law Enforcement Directive ("LED"), six of which concerned An Garda Síochána as controller.

Security breaches

The DPC handled 48 data security breach complaints during the reported period. However, the interesting, but not unexpected statistic, is the 3,542 valid data security breaches notified to the DPC during the report period. In total, 4,740 valid data security breaches were notified in the 2018 calendar year representing a 70% increase on the total number of valid data security breaches recorded in the full year of 2017. This is not surprising, as the mandatory obligation for controllers to report certain types of data security breaches only commenced on 25 May 2018. Prior to this, most reported data security breaches were made on a voluntary basis further to a non-binding DPC code.

The DPC received 92 valid data breach notifications under the ePrivacy Regulations, and 12 LED breach

notifications.

The report notes that the number of cyber security compromises notified, such as phishing, malware and ransomware attacks, increased from 49 cases in 2017 to 225 in 2018. Also, there was a reported increase in the use of social engineering and phishing attacks to gain access to ICT systems.

Cross-border processing

Under the one-stop-shop mechanism ("OSS"), the DPC is the 'lead supervisory authority' for a large number of high-profile multinationals, whose main establishment is in Ireland. During the report period, the DPC received 136 cross-border processing complaints through the OSS mechanism that were originally submitted by individuals with other EU supervisory authorities. Cross-border processing complaints regarding consent was the largest type, followed by the rights to erasure and access.

The report highlights: "the DPC is no longer a data protection authority with a purely national focus; it has become a supervisory authority with an EU-wide remit, responsible for protecting the data privacy rights of millions of individuals across the EU." The DPC notes the consequent need for close cooperation and information exchange between it and relevant EU supervisory authorities. In this regard, its OSS Operations unit use the EU IMI system to share information on cross-border cases with other EU supervisory authorities.

Investigations and enforcement

Whilst prosecutions were taken by the DPC under the ePrivacy Regulations in respect electronic direct marketing, the DPC is yet to issue any administrative fines or other sanctions under the GDPR.

By the end of 2018, the DPC had 15 statutory inquiries open in relation to multinational technology companies' GDPR compliance. 9 of these inquiries commenced in response to complaints, while the remainder were commenced at the DPC's own volition. The DPC anticipates that some of these statutory inquiries will conclude in 2019 and contribute to answering some of the complex privacy issues related to the ad tech sector.

Some things to note for 2019

- In late 2018, the DPC established an advanced technology evaluation and assessment unit, the Technology Leadership Unit ("TLU"). Since its establishment, the TLU has produced internal guidance on ePrivacy, internet protocols and data portability, ad tech and accountability. External guidance is anticipated in 2019 covering AI and machine learning, ad tech, device ID settings and cybersecurity. Also, the TLU will undertake a range of specialist external activities including compliance "sweeps" and evaluating data subjects' perspectives of controller compliance efforts through desktop surveys.
- Online behavioural advertising will come under greater scrutiny, with the ad tech sector identified as a priority for 2019.
- The DPC received 900 DPO notifications during the report period. The DPC's plans for 2019 include communicating with relevant organisations regarding their statutory obligation to appoint a DPO.
- The DPC is currently lead reviewer in relation to 11 Binding Corporate Rules ("BCRs") applications, and expects this to grow further in 2019. During the report period, the DPC was contacted by several companies considering moving their lead authority for BCR purposes from the UK to Ireland in light of Brexit.
- The DPC's large-scale consultation on the processing of children's data closes for submissions on 5 April 2019, its deadline having been extended. Following this we can expect guidance materials for children and young people, and the organisations that process their data. Also, the DPC intends to work with industry, government and voluntary-sector stakeholders and their representative bodies to encourage the drawing-up of Codes of Conduct to promote best practices by organisations that process the personal data of children and young people.
- The annual report highlights the DPC's preference for the amicable resolution of complaints, and for individuals to raise data protection concerns directly with the controller in the first instance.
- The DPC stated it will "rigorously interrogate" controllers' reliance on legitimate interests (Article 6(1)(f)) to ensure that processing conducted on this basis meets the three conditions identified by the CJEU in the Riga regional security police case.

The above is a snap-shot of some of the key issues and work-streams identified by the DPC. If you would like to know more on the issues contained in the annual report and how these may impact your business in 2019, please contact a member of our IP/IT team.

About the Author