The DPC's Annual Report — lessons to be learnt and focus for future

Victor Timon, Partner, Linda Hynes, Partner, and Audrey Whyte, Associate, Lewis Silkin, ***look at the key trends and areas of focus to emerge from the DPC's latest Annual Report***

The Irish Data Protection Commission ('DPC') recently published its Annual Report ('the Report') for 2019, covering the first complete calendar year since the General Data Protection Regulation ('GDPR') came into force. The Report provides a number of interesting insights into the DPC's activities over the past year, highlighting a number of key trends. The Report also includes information concerning the areas upon which the DPC intends to focus in the year ahead. This article discusses those key trends and areas for future focus, which should inform organisations in deepening and fine tuning their compliance strategies.

Data protection complaints

The number of complaints received by the DPC was 7,215 in 2019. This was a massive increase of 75% on the previous year. This may well have been a result of all the publicity around the coming into effect of the GDPR and data subjects' new rights. It will be interesting to see if this number tapers off in future years.

29% of the complaints related to subject access rights, although in proportion to other categories of complaints, this figure is dropping. The Report reiterates that there is a presumption in favour of disclosure on the part of controllers when handling subject access requests. Complaints relating to disclosure and fair processing made up the next highest proportion of complaints at 19% and 16% respectively.

Telcos and banks remain the most complained about sectors, with many complaints focusing on the issue of account administration and charges. (The DPC has expressed frustration that these consumer protection issues are being addressed via complaints to it, rather than being dealt with within those sectors.) Over the last year, there has been an increase in the number of complaints about internet platforms, with the key focus being on the management of individuals' accounts and the right to erasure once an individual leaves the platform.

Disputes between employees and employers or former employers 'remain a significant theme' of complaints to the DPC. The Report states that this is 'driven by the fact that neither the WRC [the Workplace Relations Commission] or the Labour Court can order discovery in employment claims', which in our experience, is probably accurate. The absence of discovery powers means that subject access requests can often play a central role in employment claims.

Data breach notifications

There were 6,069 valid data breaches notified to the DPC in 2019, up 71% from 2018. Unauthorised disclosures made up 83% of breaches, with an increase in the number of repeat breaches of a similar nature by a large number of organisations (predominantly in the financial sector). The DPC recommends that controllers take steps to mitigate the risk of data breaches, such as staff training, awareness programmes, implementing stringent password policies and multifactor authentication for remote access, and regularly updating anti-malware software.

As with complaints, this spike may have been the result of the publicity around the launch and concern about the level of fines possible. Given that concern, it will be interesting to see if the number of reported data breaches remains high as controllers report data breaches 'just to be sure'.

Data compliance investigations

In 2019, the DPC had 70 ongoing statutory inquiries, including 21 cross-border inquires. In the technology sector, the DPC is currently involved in six statutory inquiries in relation to several high-profile multinational tech companies. These inquiries related to several areas of compliance with the GDPR including:

- the lawful basis for certain data processing activities;
- compliance with the transparency principles;
- compliance with access rights; and
- the implementation of organisation

(Continued on page 10)

(Continued from page 9)

and technical measures to secure and safeguard personal data.

Investigations into 'big tech' companies progressed in 2019, with two inquiries moving from the investigative stage to a decision-making stage. We can expect to see decisions arising from these inquiries in 2020. The DPC highlights some of the complexities it faces in dealing with legal procedural issues raised during the inquiry processes (for example the application of legal privilege).

The Report also highlights the trans-national difficulties when acting as the Lead Supervisory Authority. The interaction between the different implementing laws in other countries has led to some difficulties and slowed down the investigation and enforcement process.

The Report indicates that many of these issues will be resolved following the conclusion of the first wave of statutory inquiries. In respect of the international issues, then it is expected that these will be dealt with by the European Data Protection Board.

Cookies and AdTech

One area of growing focus is the use of cookies and AdTech. In August 2019, the DPC started to examine the use of cookies and similar technologies on websites across a range of sectors to establish if organisations are complying with data protection principles (in particular the user consent requirements). User consent in compliance with the GDPR must be obtained by means of a clear, affirmative act and must be freely given, specific, informed and unambiguous. The DPC noted that many organisations use pre-checked boxes/default settings for consent to cookies and some organisations rely on the user's implied consent to cookies — neither of which are valid under the GDPR. In some instances, cookies were described as 'strictly necessary' when they palpably weren't. On some sites where there was an opportunity to opt out, the mechanisms necessary to effect those choices were not in place.

> ***"As companies like the browser, Brave, continue to pile pressure on the DPC to act on what they call a 'data free for all' operating in major tech companies, the Report warns that cookies and Adtech will be strong focus in 2020 as it seeks to ensure greater compliance in this area. Organisations who use this technology should review how it is currently being used and take any necessary action."***

The DPC says it will produce updated guidance on cookies and other technologies to take account of recent decisions from the Court of Justice of the EU ('CJEU'), such as the FashionID decision (C-40/17 of 2019).

As companies like the browser, Brave, continue to pile pressure on the DPC to act on what they call a 'data free for all' operating in major tech companies, the Report warns that cookies and Adtech will be a strong focus in 2020 as it seeks to ensure greater compliance in this area. Organisations who use this technology should review how it is currently being used and take any necessary action.

Data protection enforcement/prosecutions

Although the DPC acknowledges that the new legal framework under the GDPR will take time for organisations to implement, it notes that intensive work is underway in relation to compliance and prosecutions. As such, we can expect to see an increase in the number and level of fines imposed for non-compliance. An example of this can already be seen in the area of direct marketing offences. Those type of offences were pursued rigorously in 2019 and 165 new complaints were investigated (77 related to email marketing, 81 related to SMS marketing and seven to telephone marketing). Prosecutions were concluded against four entities in respect of a total of nine offences under the E-Privacy Regulations, with sanctions ranging from a criminal conviction and fine for repeat offenders to court ordered charitable donations in lieu of a conviction/fine for more minor breaches.

Supervision

In its supervisory role, the DPC received 1,420 general consultation queries during 2019. In the public sector, the DPC consulted with government departments on legislative proposals involving the processing of personal data, including parental leave and gender pay gap data. Recurring concerns for private sector organisations emerging from the DPC supervisory function include:

- personal data transfers following a no-deal Brexit;
- direct marketing rules under the E-Privacy Directive;
- dealing effectively with data subject access requests;
- use of technologies in the workplace such as biometric clocking/GPS vehicle tracking and CCTV;
- transfer of employee data in mergers and takeovers;
- discrepancies in privacy policies in multinational companies;
- media reports outlining security issues such as human review of voice recordings; and
- new technologies and their impact on a controller's data protection obligations.

A particular area of focus was in the Fintech and payments sector, with the advent of Open Banking and the European Payment Services Directive 2 (or PSD2) with new Fintech start-ups or trusted third-parties setting up operations in Ireland as a result. The DPC anticipates that this will 'gather momentum' in 2020, and the sharing of account information and personal data will be a 'core priority' for the DPC's consultation engagement with the private and financial sector.

Linked to its function as a Supervisory Authority, the DPC's Information and Assessment Unit was contacted almost 48,500 times, including 22,200 calls and 22,300 emails. The DPC published more online guidance to assist in interpreting the GDPR and the Data Protection Act 2018 in 2019 and intends to produce more guidance in the coming year, particularly case studies illustrating the practical application of data protection principles. Notwithstanding the increased level of guidance published by the DPC last year, it is nowhere near the level produced so far by the UK Information Commissioner's Office ('ICO'), for example. This is likely to be a resources issue.

The DPC received 712 (577 in the private sector) new Data Protection Officer ('DPO') appointment notifications from organisations in 2019, bringing the total number to 1,596. The DPC intends to mobilise its DPO network in 2020 to foster peer-to-peer engagement and knowledge sharing between DPOs. By engaging with DPOs, the hope is that the progress made to date in implementing GDPR programmes translates into lasting organisational culture and practice.

One Stop Shop for data protection complaints

The DPC is the Lead Supervisory Authority for a number of multinational corporations whose main establishment is in Ireland, and this is particularly the case in respect of the European operations of many technology and social media organisations. This means that under the One Stop Shop ('OSS') mechanism introduced by the GDPR, it has jurisdiction to manage and address data protection complaints relating to multinational corporations in other member states. Under the OSS system, the DPC must consult extensively with other Supervisory Authorities when handling regulatory matters through the OSS, and must share draft decisions relating to complaints referred or inquiries conducted under the OSS with all concerned supervisory authorities and consider their views before finalising the decision. In 2019, the DPC received 457 cross border processing complaints under the OSS which were lodged by individuals via other EU Supervisory Authorities.

Brexit and international aspects of data protection compliance

Brexit preparation has clearly created a considerable amount of work for the DPC over the last year. The DPC spent significant time engaging with stakeholders to provide information on Brexit, particularly in relation to Irish companies transferring personal data to the UK. In the area of international transfers of data, a key area of focus for the DPC has been assessing and approving Binding Corporate Rule ('BCRs'). BCRs were introduced for organisations that needed a global approach to data transfer on a large scale. In 2019, the DPC acted as lead reviewer in relation to 19 BCR applications for 12 different companies. The DPC expects this number to increase in 2020 during the post-Brexit implementation period when organisations with BCRs approved by the ICO will look to have their BCRs approved by a remaining EU Member State's Supervisory Authorities instead. In 2019, the DPC also continued to take part in various projects and programmes for international engagement and cooperation on data protection issues with other Supervisory Authorities and stakeholders.

The future focus of DPC activities

The DPC Regulatory Strategy for 2020-2025 will be published later this year. In advance of this, the DPC has engaged in focus groups with the public to establish their expectations and awareness of the DPC. The findings highlight that many people were confused about their rights and would welcome more real-world examples to understand how they apply in practice. In response, the DPC intends to produce more case studies to highlight issues from a consumer/controller point of view.

Other areas of focus for the DPC in the future include:

- continuing to prepare for the implementation of GDPR's certification approval mechanisms, which are intended to provide ways for organisations to demonstrate data protection compliance efforts to individuals;
- publishing guidance for controllers in processing children's personal data and encouraging big technology platforms to sign up to a code of conduct on children's data processing;
- continuing to expand operations. In 2019, the DPC's staffing level increased from 110 to 140 and it is likely that this number will continue to grow in 2020;
- awaiting the CJEU decision on the legitimacy of standard contractual clauses as a sufficient safeguard for the transfer of personal data;
- issuing first draft decisions on big technology companies;
- developing sector specific codes of conduct for data processing and compliance with data protection principles.

Conclusion

It is clear from the Report that as compliance with the GDPR continues to be a significant area of focus for organisations, the DPC is intensifying its efforts and expanding its operations. As a result, organisations can expect an increase in the level of the DPC's supervisory, compliance and enforcement activities.

The Report illustrates how the application of data protection principles continues to evolve to respond to developments in technology, business, social and legal practices. As such, all

(Continued on page 12)

(Continued from page 11)

organisations will need to ensure compliance with the GDPR is kept under review.

A commonality between the data breach Case Studies contained in the Report is the role played by the DPC in supporting and advising organisations on how to improve their compliance procedures, including by way of increased security or further education for relevant staff. These provide useful guidance for organisations and practical insights into how the DPC is interpreting and applying data protection principles in real life scenarios.

Helpfully, we can expect to see an increase in the amount of guidance in the coming year as a result of DPC consultations, publications and the outcome of investigations and enforcement proceedings in 2020.

Linda Hynes is leading a half day workshop on 'Data Protection and Employment — the Latest Thinking' at the 15th Annual Data Protection Practical Compliance Conference taking place in Dublin on 5th and 6th November 2020. See www.dataprotectionconference.ie for further information.

Victor Timon
Linda Hynes and Audrey Whyte
Lewis Silkin
victor.timon@lewissilkin.com
linda.hynes@lewissilkin.com
audrey.whyte@lewissilkin.com