Data Protection Commission publishes Annual Report for 2019

The Data Protection Commission (DPC) has published its Annual Report for 2019 – the first full calendar year of the GDPR.

The Report reveals some interesting statistics and trends. In particular, it highlights that during 2019, at least 40% of the DPC's resources were devoted to handling individual complaints, whilst larger-scale inquiries into multi-national technology companies also consumed considerable resources. This briefing note considers some of the highlights of the Report.

Queries

In 2019, the DPC received almost 48,500 queries from individuals and organisations. These queries included approximately 22,300 emails, 22,200 telephone calls and 4,000 items of correspondence via post. Topics of particular interest where the DPC provided support to individuals included: use of the Public Services Card; use of CCTV; access requests on behalf of children; access requests in the context of employment disputes; workplace surveillance; and photography (consent and artistic exemptions).

Complaints

The DPC received a record 7,215 complaints in 2019, which was an increase of 75% from the 4,113 complaints it received in 2018.

Data subject access requests – highest volume of complaints

The highest category of complaints continues to concern access requests (29%). A significant theme of such complaints were disputes between employees and employers. The DPC highlights that, as neither the Workplace Relations Commission nor the Labour Court can order discovery in employment claims, disgruntled employees often rely on their right of access under the GDPR. This has led to the DPC adjudicating on disputed access requests between employers and employees, and litigation being brought by individuals against DPC findings that their data protection rights were not breached. The Report notes that "*it is important for controllers to remember that the right of access is a fundamental right, so there is a presumption in favour of disclosure on the part of controllers*".

Unfair processing and unauthorised disclosure also featured heavily in the complaints received by the DPC in 2019.

Telcos & banks – most complained about sector

Telcos and banks remain the most complained about sectors, with complaints focussing on account administration and charges. Complaints about internet platforms have also grown in volume, and largely concern management of individuals' accounts and their right to erasure of their personal data when they leave a platform

Cross-border complaints – on the rise

The DPC received 457 cross-border complaints through the one-stop-shop mechanism, which were lodged by individuals with other European Data Protection Authorities (DPAs). The Report notes that although the DPC has primary responsibility for handling these complaints, it must consult extensively with the other European DPAs and keep them updated throughout its complaint handling and investigatory processes. The GDPR cooperation mechanism also requires the DPC to take account of their views and seek their consensus on draft decisions for these cross-border cases. Only three minor cross-border cases have so far resulted in fines, which were modest in size. None of those fines were issued by the Irish DPC.

Breach complaints – also on the rise

Data breach complaints from affected individuals saw a significant increase between 2018 and 2019, rising from 48 to 207. The Report notes that individuals have expressed increased dissatisfaction about the manner in which organisations have communicated with them following data breaches, and the remedial actions (or lack thereof) taken by the organisations.

Breach Notifications

The DPC received 6,069 data breach notifications, with the largest single category being unauthorised disclosures, representing 83% of all breaches. It was noted that there had been an increase in repeated breaches by certain companies, particularly those in the financial sector. Other trends identified included:

- inadequate reporting
- failure to notify affected data subjects, or a delay in reporting the breach and
- inaccurate risk assessments by data controllers

Statutory investigations

On 31 December 2019, the DPC had 70 statutory inquiries open, including 21 cross-border inquiries into multinational technology companies:

- Facebook – eight active investigations, including three separate investigations into the September 2018 'token' breach.
- WhatsApp – two active investigations, including whether WhatsApp has discharged its GDPR transparency obligations in relation to processing of information between WhatsApp and other Facebook companies.
- Apple – three active investigations, including whether Apple discharged its obligations in respect of the lawful basis on which it processes personal data for behavioural analysis and targeted advertising on its platform.
- Twitter – three active investigations, including an examination of whether Twitter has discharged its obligations in respect of the right of access to links accessed on their platform.
- LinkedIn, Quantcast, Google, Verizon, and Instagram are each subject to an ongoing investigation.

While the 21 cross-border inquiries were launched in response to a combination of user complaints and of the DPC's own volition, all 49 domestic inquiries were launched on the DPC's own volition, many in response to a data breach notification received from the company.

Of the domestic inquiries, 32 concerned surveillance for law enforcement purposes by State authorities and An Garda Síochána through technologies such as CCTV, body-worn camera, drones and other technologies. As part of the inquiry process, the DPC sought evidence of robust data protection policies as well as evidence of active oversight and meaningful governance.

The Report notes that the progression of the DPC's inquiries has given rise to procedural challenges from data controllers, as well as from individual complainants and representative bodies. The procedural challenges have included issues such as:

- How the DPC can best balance the rights and entitlements of the parties concerned in the context of requests for access to the DPC's inquiry file.
- Claims of legal privilege; confidentiality and/or commercial sensitivity over material submitted by parties to inquiries.
- Challenges to the fairness of the processes and procedures undertaken by the DPC.

The Report notes that in order to determine these issues, the DPC has had to consider how legislative provisions might be interpreted and operated in harmony with European legislation as well as how rights deriving from the EU's legal framework, such as the right of access to the file and the right to good administration, should operate in the context of an Irish regulatory inquiry. At EDPB level, EU DPAs are reportedly working together to resolve these procedural issues at a practical level to ensure the highest degree possible of harmonisation of GDPR implementation nationally.

Enforcement

The DPC has yet to conclude any of its cross-border or domestic statutory inquiries, or issue any fines or other sanctions. The DPC defends its delay on issuing any decisions or sanctions, noting that there would be little benefit in mass producing decisions only to have them overturned by the courts. The DPC states that it is "*wary of demands for quick-fix solutions and calls for the summary imposition of heavy penalties on organisations for data protection infringements…While the administrative fines mechanism represents an important element of the drive toward the kind of meaningful accountability heralded by the GDPR…enforcement…will always be subject to the due process requirements mandated by our constitutional laws and by EU law. These are constraints that cannot (and should not) be set to one side in some arbitrary fashion or for the sake of expediency*".

The DPC successfully prosecuted four entities in relation to unsolicited direct electronic marketing communications. The Report notes, for example, that complaints were made against an entity for sending unsolicited direct marketing communications and ignoring its customer's preference settings. The entity acknowledged that a large number of communications had been sent to customers who had opted out of such marketing, and that this was due to human error. As the DPC had previously prosecuted the entity for similar offences, it was convicted on five charges and fined between €750 and €1,000 for each breach of the ePrivacy Regulations 2011.

Litigation

The Circuit Court delivered two decisions in cases taken against decisions of the DPC. Although the judgments concerned the pre-GDPR regime, they provide useful guidance on data protection compliance in the post-GDPR world.

The case of *Young's Garage v The Data Protection Commissioner (4 February 2019)* concerned an appeal brought by a car dealership, against a decision of the DPC in relation to an individual's complaint against that dealership. In his complaint, the individual alleged that the dealership had provided his personal data to a third party bank to carry out a credit check without his consent. The DPC upheld the individual's complaint, finding that the dealership could not provide documentary evidence showing it had obtained the individual's consent to such disclosure. The application form which the dealership had requested the individual to complete contained a checkbox for the data subject to tick, to indicate his consent to his personal data being disclosed to the third party bank for the purposes of a credit check, but the individual had not ticked the checkbox. The dealership appealed to the Circuit Court against the DPC's decision. The Court upheld the DPC's decision, finding the dealership had not shown that it had a lawful basis for processing the data.

In *Doolin v DPC (1 May 2019)*, an employee brought an appeal against a decision of the DPC in relation to his employer's use of CCTV footage in disciplinary proceedings. Following their investigation of the complaint, the DPC found that the employer had a lawful basis to access and view the CCTV footage in order to address a potential security issue. During proceedings brought by the employee in the Circuit Court, the DPC's argument was that the further use of the CCTV footage during disciplinary proceedings was pursuant to the employer's original stated purpose, as the employee had committed a breach of security by being in an unauthorised place at an unauthorised time. This line of reasoning was accepted by the Circuit Court, and appealed to the High Court. The High Court overturned the Circuit Court decision in February 2020, finding that the DPC had made an error of law in its interpretation of "*processing*". Although the CCTV footage had not been accessed and downloaded for further use, the Judge relied on the broad statutory definition of "*processing*" to determine that the passing of information obtained from the footage constituted "*further processing*".

Case Studies

The Report contains 12 case-studies covering a broad range of data protection issues including: the right to rectification; unauthorised disclosure; consent to photography; fair processing; lawful basis; unsolicited direct marketing; and data security breaches.

Some examples include:

- **Right to rectification:** A complaint against a healthcare group for refusing to rectify the spelling of an individual's name to include an Irish accent mark (*sineadh fada*) on their computer system. The DPC consulted the Irish

Language Regulator and case law from the European Court of Human Rights on linguistic rights and naming. They noted that the right to rectification under Article 16 is not an absolute right. The primary purpose of the processing in this case (namely the administration of health care to the complainant) could be achieved without the use of diacritical marks as each patient was also assigned a unique ID number. A compromise was reached whereby a comment was added to the individual's file to show that the sineadh fada formed part of their name.

- **Consent:** Another complaint was received from a parent regarding the use of a photo of their child in promotional material. The photo had been taken by a professional photographer at a festival. Whilst the child's parent had conversed with the photographer, they had understood at the time the photo was taken that they would be contacted prior to use of their child's image. The state agency which had organised the festival indicated that they had relied on the consent obtained from the parent by the photographer, but accepted that it was not clear that the image would be used for publicity purposes. The DPC found that the parent had not been provided with adequate information in order to provide their fully informed consent for the processing of the child's image in this manner.
- **Data security:** An organisation in the leisure sector notified the DPC of a ransomware attack which had potentially disclosed the personal data of up to 500 customers and staff stored on the organisation's server. The DPC issued a number of recommendations to the organisation in relation to its IT infrastructure, and on how to ensure an adequate level of security via employee training.
- **Unauthorised disclosure:** A public sector health service provider notified the DPC that sensitive patient medical information had been discovered in an unoccupied hospital building by an intruder, who had then shared photos of the storage cabinet containing the files on social media. The DPC advised on the importance of having appropriate records management policies, and issued a number of recommendations on how to improve the organisation's personal data processing practices.

What's ahead in 2020?

2020 will be another significant year for data protection law. We await the judgment of the Court of Justice of the European Union in Schrems II, concerning the validity of standard contractual clauses as a mechanism to transfer personal data to a third country outside the EEA. We also await the first draft decisions by the DPC in respect of its statutory inquiries into multinational technology companies.

The Report indicates that the DPC hopes to move off "*first principles*" of GDPR (lawful basis/controller/processor), and really move into the meat of "*data protection by design*", to ensure the next generation of technologies complies with data protection law. In addition, the DPC will be encouraging big tech platforms to sign up to a code of conduct on the processing of children's personal data, to better protect children online.

The DPC also embarked on an operational change programme in 2019, the benefits of which are expected to be seen in 2020. Initiatives include improving the usability of web forms on the DPC website, and the introduction of a new case management system to better address operational priorities. A number of consultations were also launched in 2019 with the purpose of better understanding the public's view on data protection rights, the role of the DPC, and how compliance with data protection law should be encouraged, facilitated and maximised.

Our team

John Whelan
Partner
+353 1 649 2234
jwhelan@algoodbody.com

John Cahir
Partner
+353 1 649 2943
jcahir@algoodbody.com

Claire Morrissey
Partner
+353 1 649 2246
cmorrissey@algoodbody.com

Andrea Lawler
Partner
+353 1 649 2351
alawler@algoodbody.com

Andrew Sheridan
Partner
+353 1 649 2766
asheridan@algoodbody.com

Davinia Brennan
Associate, Knowledge Lawyer
+353 1 649 2114
dbrennan@algoodbody.com