Data Protection Commission publishes Annual Report for 2020

The Data Protection Commission (DPC) has published its Annual Report for 2020.

The Report looks back on the span of regulatory work completed by the DPC over the past year, and reveals some interesting trends and statistics. It discusses the complaints and breach notifications received by the DPC; case-studies; the 83 domestic and cross-border inquiries the DPC has open; and the fines, reprimands, and compliance orders it has issued for infringements of the GDPR and Law Enforcement Directive (**LED**). This briefing note considers some of the key highlights of the Report.

Complaints

The DPC received in excess of 35,000 data protection queries, and resolved 4,476 complaints from individuals last year. The largest categories of complaints concerned data subject access requests (**DSAR**s) (27%); fair processing (26%); unauthorised disclosure of personal data (12%); direct marketing (7%), and the right to erasure (7%).

Employment law disputes also constituted a large number of complaints. As the DPC highlighted in its Annual Report for 2019, in Ireland neither the Workplace Relations Commission nor the Labour Court can order discovery in employment claims, so 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.

Over 60% of complaints lodged with the DPC in 2020 were concluded within the same calender year. This is likely due to the DPC's increased resources. Staff numbers and budget increased in 2020 to 145 and €16.9 million, respectively (and €19.1 million in 2021).

Amicable resolution

The DPC endeavours to resolve complaints amicably, as provided for in Section 109(2) of the Data Protection Act (**DPA**) 2018. The Report highlights that the option to have complaints dealt with by amicable means is afforded to individuals throughout the lifetime of the complaint, regardless of how far the issue may have progressed through escalated channels.

The Report discusses a number of case studies in which an amicable resolution was reached. For example, *Case Study 2* discusses a complaint received by the DPC regarding a data subject's access request to an auction house. The auction house failed to respond to the request, despite the complainant issuing two subsequent reminders. The DPC engaged with the auction house who informed the DPC that while it had previously had a business relationship with the complainant in 2016, it had since deleted all the complainant's personal data. The DPC reminded the auction house of its obligation (under Article 12 and 15 GDPR) to respond to an access request within the statutory timeframe even if it is no longer in possession of the complainant's personal data.

DSARs – Legal Privilege exemption

As previously discussed, DSARs continue to constitute the largest category of complaints to the DPC. Controllers frequently assert legal privilege over documents containing personal data in order to justify refusal of an access request. The Report provides some clarity on the DPC's interpretation of the scope of the

legal privilege exemptions in the DPA 2018. Sections 162 and 60(3)(a)(iv) of the Act, restrict the right of access under Article 15 GDPR where the communications are protected by legal professional privilege. The DPC states that these provisions essentially incorporate the common law principles as they apply to privilege into the DPA 2018. At common law, legal advice privilege attaches to communications between a lawyer and client where the communication is confidential and for the purpose of giving or receiving legal advice. Litigation privilege applies to communications between a client and lawyer, or between a client and/or lawyer and a third party, where the dominant purpose of the communication is to prepare for actual or apprehended litigation.

The Report notes that where legal professional privilege is relied on to refuse an access request, the DPC will require an explanation as to why the controller is asserting privilege, and will seek a narrative of each document containing personal data.

Case Study 4 considers the scope of the litigation privilege statutory exemption. The DPC dealt with a complaint in relation to an access request that was refused by a hospital. The hospital withheld non-clinical notes containing staff statements about the complainant's care, on the basis that they were protected by litigation privilege. The DPC requested sight of the documentation on a voluntary basis, in order to be satisfied that their contents were protected by litigation privilege. The DPC concluded that the staff statements had been prepared for the dominant purpose of an internal review of the complainant's care, and no litigation had commenced or been threatened at the date of the creation of the statements. Therefore litigation privilege did not apply and the DPC directed the hospital to release the documentation.

GDPR being misused

In terms of identifiable trends, the Report highlights an increasing number of complaints that '*have little or nothing to do with data protection*', such as grievances in relation to an individual's working environment, medical treatment, or how their child was dealt with at school following an incident with another child. The DPC warns of the danger of complainants and the DPC over-reaching, noting that it may render data protection regulation meaningless, '*because it becomes the law of absolutely everything*'. In addition, individuals and organisations have been misusing the GDPR to pursue other agendas. For example, some organisations are deleting CCTV footage after they are on notice of an access request for that footage, claiming the GDPR requires them to delete it every seven days.

Cross-border complaints

The DPC, as lead supervisory authority (**LSA**), received 354 cross-border processing complaints from other EU Data Protection Authorities (**DPA**s) through the Article 60 (i.e. the one-stop-shop) procedure. In addition, it referred a number of complaints from Irish data subjects to other EU DPAs where they acted as LSAs.

For example, *Case Study 6* in the Report discusses the DPC's handling of an Irish data subject's complaint against a German-based ecommerce platform. The individual received an email from the platform notifying them that it had been hacked and that some of its users' personal information may have been leaked. The individual alerted the DPC and submitted a complaint in relation to the breach. The DPC referred the complaint to the Berlin DPA, which acted as LSA, as the company had its main establishment in Berlin. The DPC acted as a concerned supervisory authority (**CSA**), communicating with the Berlin DPA and transmitting updates in relation to the investigation (once they were translated from German to English) to the individual complainant in Ireland. The draft decision in relation to the breach described a number of measures taken by the platform to address the breach and mitigate its adverse effects, such as resetting all user passwords and ensuring new passwords were encrypted. The DPC was satisfied with the Berlin DPA draft decision and did not raise any objections. The case shows the depth of cooperation required between European DPAs under the one-stop-shop procedure.

Direct marketing complaints

The DPC investigated 147 complaints under the ePrivacy Regulations 2011 in respect of various forms of electronic direct marketing communications, including 66 email marketing; 73 text messages; and five telephone calls. The DPC prosecuted six companies in respect of

direct marketing offences under the e-Privacy Regulations. In all cases, the District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation. The court-ordered donations ranged from €200 to €5,000. The prosecuted companies were also required to pay the DPC's legal costs. All of the companies had received prior formal warning letters about direct marketing complaints, or had previously been prosecuted for direct marketing offences.

Data breaches

In 2020, the DPC received 6,628 data security breach notifications (a 10% increase on 2019 figures). 110 of these notifications (2%) were classified as non-breaches as they did not meet the definition of a 'personal data breach' as set out in Article 4(12) GDPR. The DPC concluded 90% of the total recorded breach cases in 2020 (5,932 cases).

The most frequent cause of breaches was unauthorised disclosure (86%). The DPC also saw an increase in the use of phishing attacks to gain access to the ICT systems of controllers and processors. While many organisations initially put in place effective ICT security measures, the DPC has said that organisations need to become more proactive in monitoring and reviewing the effectiveness of these measures, and provide refresher training to staff to ensure that they are aware of evolving threats.

Enforcement

Cross-border/domestic inquiries

On 31 December 2020, the DPC had 83 statutory inquiries open, including 56 domestic inquiries and 27 cross-border inquiries. A large number of the domestic inquiries concerned video surveillance of citizens by the state sector for law enforcement purposes through use of CCTV, body-worn cameras, drone and other technologies. Whilst all of the domestic inquiries are all 'own volition' inquiries, the cross-border inquiries are a mix of complaints-based (10) and 'own volition' (17) inquiries.

Cross-border/domestic decisions

The DPC used its corrective powers to issue fines, reprimands, bans and compliance orders on 11 occasions, including:

- **Tusla (Child and Family State Agency)** - The DPC imposed four fines amounting to a total of €200,000 for a number of infringements. These infringements included: failing to implement appropriate security measures to prevent the unauthorised disclosure of personal data under Article 32(1) GDPR; failing to take steps to ensure an individual under their authority does not process personal data except on their instructions under Article 32(4) GDPR; failing to report a data breach within the statutory time-frame under Article 33(1) GDPR; and failing to ensure that personal data processed was accurate and kept up-to-date under Article 5(1)(d) GDPR. The DPC also reprimanded Tusla and ordered it to bring its processing operations into compliance with the GDPR.
- **Health Services Executive (HSE)** – The DPC imposed a fine of €65,000 on the HSE for failure to implement appropriate security measures, as required by Articles 5(1)(f) and 32(1) GDPR, to prevent the unauthorised disclosure of personal data. It also reprimanded the HSE and ordered it to bring its processing operations regarding the use and disposal of hardcopy documents containing patients' personal data into compliance with the GDPR, by implementing appropriate security measures.
- **Twitter** - The DPC, acting as LSA, imposed a fine of €450,000 on Twitter, for failure to notify the DPC of a personal data breach within the statutory timeframe, and failing to adequately document the breach as required by Article 33(1) and (5) GDPR. Due to the DPC's failure to reach a consensus with the other CSAs through the Article 60 procedure, the DPC referred its draft decision to the EDPB for its binding decision under the Article 65 dispute resolution procedure. The EDPB directed the DPC to reassess the elements it relied on to calculate the amount of the fine (under Article 83(2) GDPR), and to increase the level of the fine, to ensure it was '*effective, dissuasive and proportionate*'. In its draft decision, the DPC had proposed a fine in the range of €135,000-€275,000.

- **University College Dublin (UCD)** - The DPC imposed a €70,000 fine on UCD for failing to implement appropriate security measures; storing data longer than necessary, and delaying in notifying the DPC of a data breach, contrary to Articles 5(1)(f), 32(1) and 33(1) GDPR. It also ordered UCD to bring its processing operations concerning its email service into compliance with the storage limitation principle and security requirements and issued UCD with a reprimand in respect of the infringements. The personal data breaches involved unauthorised third parties accessing UCD email accounts, and login credentials for email accounts being posted online.
- **Ryanair** – The DPC, acting as LSA, reprimanded Ryanair for infringing Article 15 GDPR, for failure to provide the complainant with a copy of a recording of a phone call following a subject access request. Due to the delay on Ryanair's part in processing the request, it had deleted the recording since the request. The DPC also found that Ryanair infringed Article 12(3) GDPR by failing to provide the complainant with information on action taken in relation to their request within the one month statutory timeframe.
- **Groupon** - The DPC, acting as LSA, reprimanded Groupon, for infringing the data minimisation principle in Article 5(1)(c) GDPR, by requiring the complainant to verify their identity by submitting copy of a national ID document. The requirement applied when data subjects made an erasure request, but not when data subjects created a Groupon account. The DPC concluded that a less data-driven solution to identity verification was available to Groupon. The decision also found that Groupon infringed Article 12(2) by requesting additional information as to the complainant's identity at the time he made his request for erasure, in circumstances where it had not demonstrated that reasonable doubts existed concerning the complainant's identity. It also infringed the data subject's right to erasure under Article 17(1)(a) GDPR, and infringed Article 6(1) GDPR by continuing to process the complainant's personal data without a lawful basis, following its receipt of a valid erasure request.
- **Kerry County Council** – The DPC used its corrective powers in respect of infringements of the LED. It found the Council did not have a lawful basis for its use of CCTV to detect litter offences. Other infringements related to appropriate signage and general transparency; lack of written rules or guidelines governing staff access to the CCTV; the use of smartphones or other recording devices in the CCTV monitoring room; and the practice of sharing login details for accessing CCTV footage. The DPC imposed a temporary ban on the processing of personal data through CCTV cameras for law enforcement purposes. It also reprimanded the Council, and ordered it to bring its processing operations into compliance.
- **Waterford City and County Council** – The DPC used its corrective powers in respect of infringements of both the GDPR and the LED. It found the Council had infringed Article 24(1) GDPR by processing personal data by means of body worn cameras prior to implementing a data protection policy for their use. It also infringed section 75 of the DPA 2018 by processing personal data by means of CCTV dash cams, covert cameras and drones prior to implementing data protection policies for their use. The DPC imposed a temporary ban on the processing of this personal data; reprimanded the Council, and ordered it to bring its processing operations into compliance.

Litigation

The Report provides details of judgments delivered and/or final orders to which the DPC was a party. The headline case in which the DPC was involved in was *Schrems II* (discussed at Appendix 5 of the Report). The Court of Justice of the European Union (**CJEU**) declared the EU-US Privacy Shield invalid, and the Standard Contractual Clauses (**SCC**s) valid, subject to certain conditions (previously discussed here). Following the CJEU's judgment, the DPC initiated an inquiry into Facebook's transfers to the US. This inquiry was subject to judicial review proceedings by Facebook, which was heard by the High Court in December 2020. Judgment is awaited.

Another notable decision was the Court of Appeal's ruling in *Nowak* v *DPC*. The Court held that while the definition of "*personal data*" is very broad, to

interpret a document as constituting personal data for the sole reason that it was generated as a result of a complaint made by the data subject, would be to "*overstretch*" the concept of personal data. In a related judgment, the Court found that the data subject was entitled only to a "*copy*" of his personal data, and not the data in its "*original*" (previously discussed here).

In addition, in *Doolin* v *DPC*, the High Court held that an employer's use of CCTV footage in an employee's disciplinary proceedings constituted unlawful further processing. The Court found that the CCTV footage was lawfully collected for security purposes. However, the CCTV footage was then unlawfully further processed for the purpose of the disciplinary proceedings. The decision shows the importance of only using personal data, particularly CCTV footage, for the purpose for which it was collected (previously discussed here).

What's ahead in 2021?

The DPC will continue to have a leading profile in relation to international enforcement as it completes further cross-border inquiries into multinational technology companies and exercises its corrective powers. Although the decisions in Ryanair, Groupon and Twitter show the lengthy time it can take for decisions to be finalised following the Article 60 (i.e. one stop shop) procedure.

We will undoubtedly see further regulatory activity at Irish and EU level in respect of international transfers of personal data. The European Commission's draft SCCs address the CJEU's decision in Schrems II and are expected to be finalised in the coming months. We also await the European Commission's adoption of a UK adequacy decision. The Cooperation and Trade Agreement provides a temporary solution to the issue of the UK becoming a third country on 31 December 2020, by allowing personal data to continue to flow freely from the EU to the UK until 30 June 2021 or until the EU Commission adopts a UK adequacy decision (whichever is sooner). In mid-February 2021, the EU Commission delivered a draft UK adequacy decision, which has yet to be approved by the EDPB, and by a committee of representatives from EU Member States.

We may also see further enforcement of the rules on cookies. Last year, the DPC published new guidance in relation to the use of cookies and tracking technologies, and signalled its intention to begin enforcement action during Q4 of 2020. In December 2020, the DPC served Enforcement Notices on seven website operators for non-compliance with the rules on cookies.

In addition, the DPC has announced that it will expand its regulatory activities in relation to compliance by *private sector* organisations with Article 37 GDPR (where applicable). That provision sets out an obligation for certain organisations to designate a Data Protection Officer and communicate their details to the DPC. In 2020, the DPC commenced a project to assess compliance by *public bodies* with their Article 37 GDPR obligations. From a total of almost 250 public bodies, the DPC identified 77 public bodies as potentially not compliant with the requirements in Article 37 GDPR.

Our team

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

John Cahir
Partner
+353 1 649 2943
jcahir@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