TECHNOLOGY

The Data Protection Commission's 2019 Annual Report at a Glance

February 2020

On 20 February 2020, the Data Protection Commission launched its 2019 Annual Report, the first report covering a full year of GDPR activity.

AWARDS

Ireland M&A Legal Adviser of the Year 2019
Mergermarket European M&A Awards

Best Firm in Ireland 2019
Europe Women in Business Law Awards

Best National Firm for Women in Business Law 2019
Europe Women in Business Law Awards

Best National Firm Mentoring Programme 2019
Europe Women in Business Law Awards

Best National Firm for Minority Women Lawyers 2019
Europe Women in Business Law Awards

Ireland Law Firm of the Year 2019
Who's Who Legal

European Finance Deal of the Year 2019 (NTMA Green Bond Transaction)
The Lawyer European Awards

Most Inclusive Law Firm 2019
Managing Partners' Forum Awards

Here are some of the more notable highlights:

Statutory Inquiries

- At the end of 2019 – DPC had 70 statutory inquiries open (21 of which were cross-border);
- Multinational technology company inquiries commenced in 2019 include investigations of Facebook, Apple, Twitter, Quantcast, Google and Verizon Media/Oath.
- Domestic own volition inquiries commenced in 2019 include investigations of Bank of Ireland, the Catholic Church, SUSI, Irish Prison Service, Maynooth University and TUSLA amongst others.

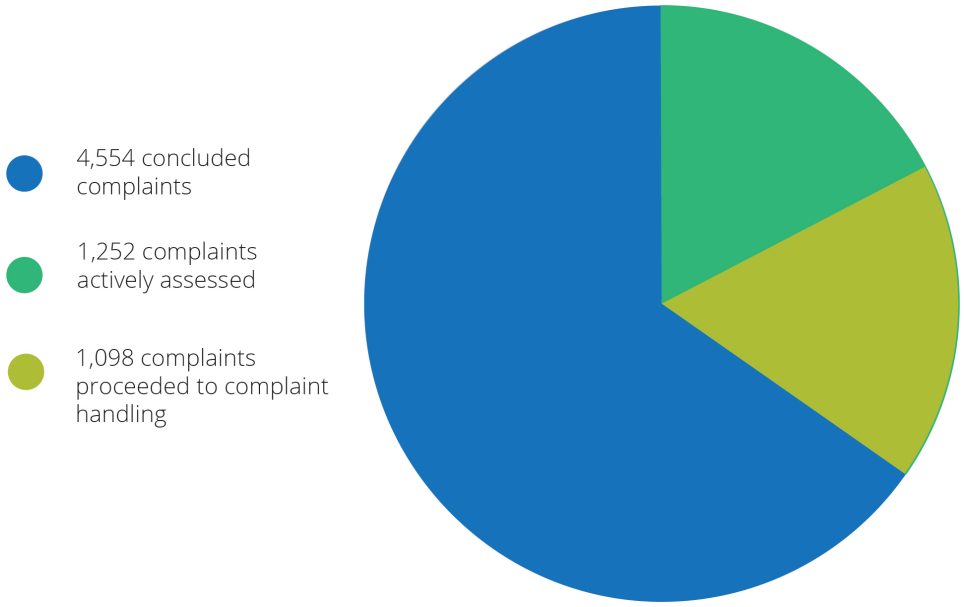
Complaints

- 7,215 complaints received (nearly doubled from 2018);
- 457 cross-border complaints initiated through the One-Stop-Shop process.

Top 5 complaints representing 76% of total complaints received under the GDPR

Data Subject Access Requests (DSAR)	29%
Disclosures	19%
Fair processing of data	16%
E-marketing	8%
Erasure	5%

As of 31 December 2019



Data Breach Notifications

- 6,257 data breach notifications received (a 71% increase from 2018);
- Unauthorised disclosure represented 83% of all breaches.

Top 5 breach notifications representing 95% of all breach notifications

Unauthorised disclosure	5,188
Paper lost or stolen	345
Phishing	161
Unauthorised access	131
Hacking	108

Case Studies

1. Right to rectification request to a healthcare group

The complainant alleged that a healthcare group was incorrectly spelling his name on its computer system by not including the síneadh fada, an accent forming part of the written Irish language. The DPC examined the healthcare group's language scheme, as well as the costs which may be incurred or errors which may be caused in updating the group's computer systems to support the use of the fada in identifying patients. The DPC found that cross-system handling of the síneadh fada would increase the risk to the complainant and impact any health-care decisions made in respect of this individual. Therefore in the circumstances, the non-use of the síneadh fada did not constitute an interference with the fundamental rights of the individual.

2. Telecommunications company discloses data to former employer

The telecommunications company, as data controller, failed to take the required action to reflect the change in circumstances that was notified to it by the complainant when she requested the restriction and separation of her account from that of her former employer. The DPC found that the telecommunications company did not implement appropriate security measures to protect the complainant's personal data from unauthorised access by, and disclosure to, her former employer. It also did not put in place effective training for its employees in this regard. Additionally, the fact that the company could not locate the complainant's initial account restriction request meant that it had failed in its obligation to keep her records accurate, complete and up-to-date.

3. Lack of consent to use festival child's photo for PR purposes

While a parent had consented to their child's photograph being taken at a festival, it had not been made clear to the parent that this image may later be used for media/PR purposes.

The DPC found that the State Agency involved in organising the festival had not provided the child's parent with adequate information in order to consent to the processing of the image used in promotional material.

4. Private receivers may process the personal data of borrowers in order to manage and realise secured assets
This case study provided welcome clarity on the complex area of receiverships. The case study clarifies the DPC's views on a number of items:

- A newly-appointed receiver was not required to register as a data controller under the pre-GDPR registration rules, as it could rely on an exemption afforded to data controllers for the processing of the personal data of their customers.
- The receiver had a lawful basis for obtaining the complainant's personal data from the relevant financial institution, as this processing was necessary for the performance of the mortgage contract. The receiver could lawfully disclose personal data to its managing agent as this data had been obtained for the explicit purpose of entering into a loan agreement.
- The opening of a bank account by the receiver was a reasonable measure to manage the income and expenditure during the receivership. Reference to the complainant's name on the bank account was necessary to ensure that the receivership was carried out efficiently.
- However, the receiver should have given the complainant a broad outline of the purposes for which the personal data was intended to be processed, as well as the categories of personal data it held in relation to the complainant.
- The decision is currently the subject of an appeal to the Circuit Court.

5. Direct marketing complaints
The Annual Report contains the usual run through of prosecutions undertaken by the DPC in connection with ePrivacy offences relating to direct marketing activities. Companies prosecuted in 2019 were from a range of industries, including telecoms, food delivery services and online retailing. The activity prosecuted covered unsolicited emails and SMS messages where the sender did not have the requisite level of consent required by Regulation 13 of SI 336 of 2011. As is usually the case, the unlawful activity arose through a variety of human and system failures and the DPC continued its "two strikes" policy of prosecuting on foot of a valid second complaint.

6. Data breach complaints
An individual complained to the DPC that their personal data around attendance at a pregnancy unit of a hospital was disclosed via Facebook Messenger by a hospital porter. The HSE explained the porter was a contractor from a health agency. The DPC sought an update on the agency's internal investigation and simultaneously advised the HSE that it was ultimately the data controller for personal data in this instance. The complaint was subsequently withdrawn following a settlement agreement with the hospital. The DPC report reminds readers that it has no role in compensation claims and so had no further involvement. However, the DPC emphasised the importance of ongoing training and diligence by data controllers.

7. Data breach notifications
The Annual Report reviews a number of different categories of data breaches which arose in 2019:

Loss of control of paper files: The DPC was notified by a health service provider that a number of files with medical data were found in a storage cabinet on a hospital premises which was no longer occupied. The records were discovered by someone who illegally accessed the premises and put pictures of the cabinets on social media. A representative of the health service provider was sent to locate and secure the files. The files were removed and stored. The case highlights the importance of appropriate record management policies and the DPC issued a number of recommendations to the organisation.

Ransomware Attack: An organisation in the leisure industry was the victim of an attack which potentially disclosed the personal data of up to 500 customers and staff on the organisation's server. The modem router had been comprised. Back up data was stored securely via a cloud server. The DPC issued a number of recommendations to the organisation, including an analysis of the ICT infrastructure to ensure an adequate level of security against further malware, and employee training for cyber security risks. The DPC has received regular updates and is satisfied that the organisation is taking steps to improve its organisational and technical measures including the development of a suitable training programme.

Disclosure of CCTV footage via social media: An employee of a security company who had been contracted by a property management company used their mobile phone to record CCTV footage of two individuals engaged in an intimate act. This employee shared the footage on WhatsApp. The property management company communicated to staff that if they received the footage, they must delete it immediately. The property management company and the security company both demonstrated that adequate policies and procedures existed but appropriate oversight and supervision of these policies and procedures was lacking. Following recommendations made by the DPC, the property management company has engaged with staff and delivered further training. Signs have been displayed prohibiting the use of personal devices in the CCTV control room.

What is in store for 2020?

The Annual Report reflects the increased activity of the DPC in the past year across a range of areas. Their staff has grown from 110 to 140 in that timeframe and its overall budget was increased to €15.2 million. During this timeframe, the DPC has come under increasing pressure to deliver decisions in relation to its higher profile cross-border investigations. However, the Report points out that the detailed process to be followed under the Data Protection Act 2018 along with the One Stop Shop process that applies for most of those cases inevitably results in delays. The Report notes that

"the DPC anticipates that 2020 will involve the reconciliation of many such complex legal issues which will flow from the conclusion of its first waves of statutory inquiries (particularly those which must progress to final resolution under the One Stop Shop mechanisms i.e. where the DPC is the Lead Supervisory Authority) and the crystallisation in practical terms of many theoretical legal and procedural issues which have been raised during those first novel inquiries."

One can therefore expect the 2020 Annual Report to include the first decided cases by the DPC on those high profile cases. It would be surprising if we did not by then have a good sense of the DPC's views on what constitutes an "effective, proportionate and dissuasive" fine under Article 83 GDPR.

The authors wish to thank Bronágh Carvill, Valentyna Chekanska and Clíodhna Ní Ghadhra for their contribution to this briefing.

OUR DATA PROTECTION TEAM

Rob Corbet
Partner
+353 1 920 1211
rob.corbet@arthurcox.com

Colin Rooney
Partner
+353 1 920 1194
colin.rooney@arthurcox.com

Olivia Mullooly
Partner
+353 1 920 1060
olivia.mullooly@arthurcox.com

Pearse Ryan
Consultant
+353 1 920 1180
pearse.ryan@arthurcox.com

Dr Robert Clark
Consultant
+353 1 920 1231
bob.clark@arthurcox.com

Ciara Anderson
Associate
+1 415 829 4247
Ciara.Anderson@arthurcox.com

Eoghan Clogher
Associate
+353 1 920 1405
Eoghan.Clogher@arthurcox.com

Ian Duffy
Associate
+ 44 207 832 0217
Ian.Duffy@arthurcox.com

Colm Maguire
Associate
+353 1 920 1416
Colm.Maguire@arthurcox.com

Hugh McCarthy
Associate
+353 1 920 1324
Hugh.McCarthy@arthurcox.com

Caoimhe Stafford
Associate
+353 1 920 1328
Caoimhe.Stafford@arthurcox.com

Aoife Coll
Associate
+353 1 920 1726
Aoife.Coll@arthurcox.com

Rachel Benson
Professional Support Lawyer
+353 1 920 1435
Rachel.Benson@arthurcox.com