TECHNOLOGY AND INNOVATION

The Data Protection Commission's 2020 Annual Report at a Glance

March 2021

In the year of the first DPC fines under the GPDR there were also increases in numbers of open statutory inquiries and breach notifications while the number of complaints decreased.

On 25 February 2021, the Data Protection Commission published its 2020 Annual Report. Here are some of the more notable highlights:

DECISIONS

ENTITY	CORRECTIVE POWERS EXERCISED	FINE(S)
Kerry County Council	• Temporary ban on processing • Order to bring processing into compliance (specified actions) • Reprimand – Art. 6	N/A
Tusla (Child and Family Agency) (1)	• Order to bring processing into compliance (technical & organisation measures) • Reprimand – Arts. 32(1) & 33(1)	€75,000
Tusla (Child and Family Agency) (2)	• Order to bring processing into compliance (technical & organisation measures) • Reprimand – Arts. 32(1) & 33(1)	€40,000
Tusla (Child and Family Agency) (3)	• Order to bring processing into compliance (disposal of patient records) • Reprimand – Arts. 5(1)(d), 32(1), 32(4) & 33(1)	€50,000 & €35,000
Health Service Executive	• Order to bring processing into compliance (technical & organisation measures) • Reprimand – Arts. 5(1)(f) & 32(1)	€65,000
Waterford City and County Council	• Temporary ban on processing, order to bring processing into compliance • Reprimand – Art. 6 and s. 769 DPA	N/A
Ryanair	• Reprimand – Arts. 12(3) & 15	N/A
University College Dublin	• Reprimand – Arts. 5(1)(f) & 32(1))	€70,000
Groupon	• Reprimand – Arts. 5(1)(c), 6(1), 12(2) & 17(1)(a)	N/A
Twitter	• Reprimand – Arts. 33(1) & 33(5)	€450,000

We will shortly publish a briefing analysing the various published DPC decisions to date.

STATUTORY INQUIRIES

- At the end of 2019 – DPC had 83 (up from 70 in 2019) statutory inquiries open (27 of which were cross-border);
- Multinational technology company inquiries commenced in 2019 include investigations of Facebook, Apple, Twitter, LinkedIn, Quantcast, Google, MTCH, Yelp and Verizon Media/Oath.
- Domestic own volition inquiries commenced in 2019 included investigations of:
  - Private Sector (Bank of Ireland, BEO Solutions, Slane Credit Union)
  - State/Public Agencies (SUSI, Department of Social Protection, Irish Prison Service, Tusla, An Garda Síochána, HSE)
  - Universities (NUI Maynooth, UCD and University of Limerick).

COMPLAINTS

- 4,660 (down from 7,215 in 2019) complaints received;
- 354 (down from 457 in 2019) 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)	27%
Fair processing of data	26%
Disclosure	12%
Direct marketing	7%
Erasure	7%

DATA BREACH NOTIFICATIONS

- 6,628 (up from 6,257 in 219) data breach notifications received;
- Unauthorised disclosure represented 86% of all breaches.

Top 5 breach notifications representing 95% of all breach notifications

Unauthorised disclosure	5,837
Paper lost or stolen	275
Unauthorised access	146
Hacking	146
Phishing	74

CASE STUDIES

Domestic

1. **Unauthorised publication of a photograph (Amicable Resolution)**
   A public sector employer shared a photo of an employee in a workplace newsletter. The DPC suggested Amicable Resolution ("**AR**") and the employer issued an apology which was not deemed sufficient by the employee. The DPC provided recommendations for a consent leaflet which the employer implemented. As the DPC were satisfied with these measures it issued a letter stating that the employer had processed data without consent and closed the case.
2. **No response received to subject access request (Amicable Resolution)**
   An individual requested all personal data relating to them from an auction house platform and did not receive a response. The DPC suggested the AR process and it was shown that the auction house had deleted all personal data relating to the individual. While it no longer held such data, the auction house was still obliged to respond to the individual pursuant to Article 12(3) within the required timeframe. The DPC provided guidance to the auction house on this subject.
3. **Retention of a minor's personal data by a State Agency (Amicable Resolution) (Applicable Law — Data Protection Acts, 1988 and 2003)**
   An Irish state agency was requested to delete a file relating to an incident involving a child at school which the agency had decided was did not warrant further investigation. The agency had a policy of retaining such data until the child reached the age of 25 years but following an AR process the state agency agreed to delete the file.
4. **Legal Privilege invoked to withhold personal data (Access Request Complaints)**
   An individual requested copies of personal data from a hospital arising from the care they received. The hospital released some information but withheld other information on the ground of litigation privilege. The view of the DPC was that in circumstances where the information had been prepared for the dominant purpose of an internal review and no litigation had commenced or been threatened at the date of the creation of the statements that litigation privilege would not apply and so it directed that they be released.
5. **Attendance Monitoring and Facial Recognition at a secondary school (Direct Intervention)**
   Following a meeting with the DPC the Board of Management of a secondary school decided not to proceed with a trial of facial recognition for attendance. The DPC outlined concerns in relation to purpose limitation, data minimisation, special category data and DPIAs.
6. **Purpose Limitation in the context of the Law Enforcement Directive ("LED")**
   The DPC found that data protection legislation did not disallow the separate referral by the Department of Agriculture, Food & the Marine ("**DAFM**") of allegations of professional misconduct to the Veterinary Council of Ireland in relation to a person, in tandem with prosecution proceedings by DAFM against the same individual for offences in the equine and animal remedies area, as Section 71(5) DPA 2018 provided a basis for the processing. Sections 69 to 104 of the DPA 2018 give effect to the LED in Ireland.
7. **Alleged disclosure of the complainant's personal data by a local authority (Data Breach Complaint)**
   After an unsuccessful AR process with a local authority in which the complainant refused to engage in the process, the DPC found that the personal data were not processed by the local authority in a manner that ensured appropriate security of the personal data and that an unauthorised disclosure of the complainant's personal data, constituting a personal data breach, had occurred. After consultation with the local authority the DPC did consider further action as being necessary.

Cross-Border

8. **Handling an Irish data subject's complaint against German-based Cardmarket using the GDPR One Stop Shop mechanism (Applicable law — GDPR & Data Protection Act 2018)**
   An Irish individual made a complaint to the DPC against Cardmarket, a German based e-commerce platform after the individual received notice of a data breach in which their personal data was breached. The DPC engaged with the Berlin DPA under the One-Stop-Shop ("**OSS**") mechanism and the Berlin DPA released two decisions: one on the wider breach and another on the complaint to the DPC. After reviewing the Berlin DPA decision the DPC concluded that no clarifications or requests for amendment were required, thus concluding the OSS process.
9. **The Operation of the Article 60 Procedure in Cross Border Complaints: Groupon**
   The DPC received a complaint via the Polish DPA from an individual concerning Groupon's practice at the time of requiring data subjects to verify their identity with an electronic copy of a national identity card. This requirement applied when individuals made certain requests, including requests for erasure of personal data, but the requirement did not apply when individuals created a Groupon account. The DPC reprimanded Groupon for a number of infringements of the GDPR. This case study also provides a helpful summary of the Article 60 cooperation procedure.
10. **Amicable Resolution in Cross Border Complaints: MTCH**

A complaint relating to a user requesting erasure, after being banned from dating app Tinder, was amicably resolved after an investigation by Tinder found that the user had been banned for suspected infringement of terms due to the particular custom build of Android that the user was accessing the Tinder app from, rather than the user actually engaging in conduct that contravened the app terms. Following the AR process the DPC opened a separate statutory inquiry into related privacy concerns about the Tinder app.

11. **Amicable Resolution in Cross Border Complaints: Facebook Ireland**

Following an AR process a complainant was able to verify his identity with Facebook in order to request erasure of all personal data held by Facebook regarding him. Interestingly the DPC noted that the case raises the question of whether a controller should have been capable of resolving such matters without the requirement for extensive DPA-resources to mediate the outcome.

12. **Article 60 Non-response to an Access Request by Ryanair**

Following a complaint passed to the DPC from the ICO, and an unsuccessful AR process, Ryanair were found to have not fully complied with an access request. In another interesting observation on the Article 60 procedure, the DPC noted that this case study demonstrates that,

where a complaint relating to the cross border processing of personal data cannot be amicably resolved, the Article 60 procedure that follows as a result is particularly involved, complex and time-consuming. In this case, the initial draft of the DPC's decision was uploaded to the IMI on 25 May 2020, and the final decision was not adopted until 11 November 2020, some six months later.

13. Breach Case Studies

- **Breach Notification (Voluntary Sector) — Ransomware Attack**

  The DPC received a breach notification from an Irish data processor and an Irish data controller who had engaged this processor to provide webhosting and data management services. The breach related to a ransomware attack that occurred in the data centre utilised by the data processor. The DPC engaged with both parties on issues such as the processor's use of a data centre in the US to store back-up data without adequate agreements and sufficient oversight by the controller over its processor. The DPC concluded this case by issuing recommendations to both controller and processor.

- **Breach Notification (Public Sector) Erroneous Publication on Twitter**

  A public sector organisation notified the DPC that they had inadvertently published personal data via their social media platform. The root cause of this incident was human error and the offending tweet was removed without undue delay. The DPC issued a number of recommendations centring on the appropriate use of social media platforms and how social media accounts should be secured and limited to a specified number of authorised personnel.

- **Breach Notification (Financial Sector) Bank Details sent by WhatsApp**

  A private financial sector organisation notified the DPC that a member of staff used their personal mobile phone to send a picture of what they believed to be information requested by a customer over a messaging platform. However, the staff member erroneously sent details pertaining to another customer to the requesting customer. The DPC issued a number of recommendations including the use of only approved organisational communication tools, making staff fully aware of acceptable and non-acceptable behaviour when using organisational communications tools, and a recommendation to ensure staff have undergone appropriate training.

- **Breach Notification (12 Credit Unions) Processor Coding Error**

  The DPC received separate breach reports from 12 credit unions that employed the services of the same processor which was based in the UK. The breach by the processor arose from a coding error made by the processor which resulted in an indication that the borrowers affected had undergone a "restructuring event". The credit unions in question became aware of the processor's coding error several weeks after the breach. The DPC highlighted the importance of processing contracts that properly implement the requirements of Article 28 of the GDPR. In particular, processing contracts must provide for the processor to assist the controller in meeting its obligations for security of processing, and for reporting and responding to breaches.

Supervision

14. Vodafone seeks employment details from customers

The DPC received a number of queries from Vodafone customers regarding requests to produce their employment details as a requirement for the provision of service by the company. The concerns raised by the DPC included that the processing did not comply with the principles of lawful, fair and transparent data collection, data minimisation, purpose limitation principle and transparency. The company admitted that it had made an error in the collection of this information which was caused by a legacy IT system that had not been updated to remove this requirement and immediately commenced a plan to remediate the problems caused.

15. Facebook Dating

In February 2020, the DPC was informed of Facebook's impending launch of 'Facebook Dating' in the EU. Facebook hosted a DPC on-site inspection at their offices to allow the DPC to obtain more documentation and information. A number of concerns identified by the DPC were put to Facebook on the new product. As a result Facebook provided detailed clarifications on the processing of personal data and made a number of changes to the product prior to ultimately being launched in the EU in October 2020. The changes included clarifications on the uses of special category data and greater transparency.

16. Facebook Suicide and Self-Injury feature

In 2019, Facebook informed the DPC of their plans to expand the use of its Suicide and Self Injury Prevention Tool. Facebook intended that the tool would help identify users at risk of suicide or self-harm. The DPC raised a number of concerns including lawful basis and adequate safeguards relating to the processing of special category data. In 2020, Facebook proposed a more limited use of this tool for the sole purpose of removing content contravening Facebook Community Standards and Instagram Community Guidelines. No significant concerns were identified by the DPC so long as the processing was for the sole purpose of content moderation.

17. Facebook Election Day Reminder

In advance of the Irish General Election in February 2020 the DPC notified Facebook that the Facebook Election Day Reminder feature raised a number of data protection concerns particularly around transparency to users about how personal data is collected when interacting with the feature and subsequently used by Facebook. Facebook responded to the DPC advising that it intended to withdraw the roll-out of the EDR function for the election as it was not possible to implement changes in advance of the Irish election.

18. Google Voice Assistant Technology

The DPC engagement with Google on the company's voice assistant product continued in 2020. The DPC sought a response from Google on the further actions that could be taken by Google to mitigate against risks to the personal data of users, particularly arising from misactivations of Google assistant. Google has implemented a number of changes to address the concerns raised, including (i) a new transparent user engagement and consent flow; (ii) measures to decrease misactivations; and (iii) deletion of a user's Assistant interactions by voice command on Assistant.

WHAT IS IN STORE FOR 2021?

The Annual Report reflects the increased activity of the DPC in the past year across a range of areas. Their staff has grown again to 145 with two recruitment competitions ongoing as of December 2020 and its budget was increased to €16.9 million making it one of the top-three resourced DPAs per capita. During recent months, the DPC has come under increasing pressure to deliver decisions in relation to its higher profile cross border investigations. However, the Report and some of the case studies outline the

detailed process to be followed under the Data Protection Act 2018 along with the One Stop Shop mechanism that applies for most of those cases and illustrates the inevitably of delays resulting from those processes.

As expected, several of the DPC's large-scale inquiries were concluded in 2020 with decisions being published. The DPC noted that "*a number of the inquiries that progressed in 2020 were cross-border in nature and so, as required by the Article 60 procedure laid down in the GDPR, the DPC transmitted a draft decision for consideration by its fellow EU supervisory authorities before the decision could be finalised.*" The Twitter decision was the first look at what the 2019 DPC Report described as "*the crystallisation in practical terms of many theoretical legal and procedural issues which have been raised during those first novel inquiries*" and gives a valuable insight into what is to come in 2021.

One can therefore expect the 2021 Annual Report to include a significant number of decided cases by the DPC on those high profile cases. While 2020 gave us a taste of the DPC's views on what constitutes an "effective, proportionate and dissuasive" fine under Article 83 GDPR, 2021 is likely to give us a fuller understanding of the corrective powers and administrative fines that the DPC will utilise in the coming years.

OUR 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

Ian Duffy
Associate
+353 1 920 2035
Ian.Duffy@arthurcox.com

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

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

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

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

Siobhán O'Shea
Associate
+353 1 920 1839
siobhan.oshea@arthurcox.com

Alison Peate
Associate
+353 1 920 1828
alison.peate@arthurcox.com

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