

ANNUAL REPORT

2020



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Table of Contents

Glossary	3
Foreword	4
Executive Summary	8
1. Roles and Responsibilities	12
2. Contacts, Queries and Complaints	14
3. Breaches	36
4. Inquiries	42
5. Decisions	48
6. Other Investigations and Enforcement Actions.	54
7. Legal Affairs	56
8. Supervision	62
9. Data Protection Officers	70
10. International Activities	72
11. Key DPC Projects	74
12. Communications	76
13. Corporate Governance	78
Appendix 1: Report on Protected Disclosures received by the Data Protection Commission in 2020	82
Appendix 2: Report on Energy Usage at the DPC	84
Appendix 3: Prosecutions in relation to electronic direct marketing complaints	85
Appendix 4: Twitter International Company – Inquiry (IN-19-1-1) under Section 110 of the Data Protection Act 2018.	87
Appendix 5: Litigation concerning Standard Contractual Clauses.	90
Appendix 6: Financial Statements for the Year 1 January to 31 December 2020 and the DPC’s Statement of Internal Controls	98

Glossary

AG — Advocate General

BIIDPA — British, Irish and Islands' Data Protection Authorities

CJEU — Court of Justice of the European Union

CSA — Concerned Supervisory Authority

DPA — Data Protection Authority

DPC — Data Protection Commission

DPIA — Data Protection Impact Assessment

DPO — Data Protection Officer

EDPB — European Data Protection Board

GDPR — General Data Protection Regulation

IMI — Internal Market Information System

LED — Law Enforcement Directive

LSA — Lead Supervisory Authority

OSS — One Stop Shop

SCCs — Standard Contractual Clauses

SMC — Senior Management Committee



Foreword

Introduction

2020 was the second full year of application of the GDPR and the Law Enforcement Directive (LED).

This annual report details the extensive span of regulatory work completed by the Data Protection Commission (DPC) in 2020 in the discharge of its wide-ranging role in overseeing and regulating the application of EU data protection and e-privacy laws. During this period, the DPC has continued to drive compliance and accountability by organisations with their obligations under the EU's legal framework for personal data processing. In particular, the DPC has progressed over the last year definitive interpretations of key principles and requirements of EU data protection law through a range of enforcement actions and through the conclusion of the proceedings the DPC initiated in 2016 in the High Court seeking a reference to the Court of Justice of the European Union in relation to EU to US personal data transfers. While transfers of personal data occur from every EU member state to the US, the DPC has made a unique contribution as a data protection authority in bringing clarity to and pursuing enforcement of this aspect of EU data protection law.

Large-scale inquiries

A headline feature of the GDPR in replacing the previous EU Directive were the dissuasive enforcement tools it offered to deal with cases posing significant risk to EU data subjects, including arising from intentional or negligent behaviour on the part of organisations. Accordingly, the DPC has pursued a range of cases to establish whether infringements of the GDPR were occurring and what actions and sanctions would be necessary to remedy any such infringements found. Several of the DPC's large-scale inquiries were concluded in 2020. Each inquiry concluded with a detailed decision, the identification of infringements in many cases and the imposition of a range of corrective measures including fines arising from the assessment of those infringements.

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. In the case of Twitter International Company, a final decision was issued through the Article 60 procedure. This decision provided an important analysis of the data breach notification and documentation requirements imposed on organisations by Article 33 GDPR (a detailed

summary of that case can be found in the Appendix). Separately, a draft decision was also submitted to the Article 60 procedure by the DPC in the case of WhatsApp's compliance with its transparency obligations under the GDPR. That draft decision is currently progressing through the co-operation procedure at EU level. Cross-border cases in relation to Ryanair and Groupon were also concluded through Article 60 by DPC in 2020.

As the pipeline of inquiries being concluded by DPC continues to yield final detailed decisions, it assists all organisations in their understanding of how the law applies. These large-scale inquiry cases are detailed in chapter four of the report.

Law Enforcement Directive (LED)

A sufficient number of inquiries have also now been concluded under the LED to support a view that there has been significant under-engagement with — and implementation of — the requirements of the Law Enforcement Directive in Ireland. This perhaps reflects the dominant nature of the preparations relevant organisations were making for the more general framework law (the GDPR). Nonetheless, this is an important area of protection of rights that requires personal data processing for law enforcement purposes to be specified in terms of its objectives and purposes in law. The outline of the DPC decisions arising from inquiries in respect of personal data processing by local authorities and An Garda Síochána in chapter 6 of this report illustrate the point.

Complaints

Aside from the larger-scale inquiries, day-to-day work in handling the tens of thousands of queries to the office from organisations and individuals continued throughout 2020 serviced by an expanded and dedicated team at the DPC. 4,476 complaints against organisations from individuals were resolved last year. The complaints raised by individuals ranged from issues with securing access to their personal data from all types of organisations, to complaints about excessive personal data collection, to unauthorised and unnecessary disclosure of personal data to third parties. Cases concerning employment law disputes continue to be heavily represented in the range of complaints we received.

In terms of identifiable trends, it's becoming an increasing feature of the complaints received by the office that issues are being raised with the DPC that, in truth, have little or nothing to do with data protection. While the DPC delivers meaningful and effective outcomes in those cases where an identifiable data protection issue is discernible from the complaint received, the DPC is concerned that the overall volume of complaints it receives — a growing number of which disclose no identifiable data protection issue at all — reflects a desire on the part of many individuals to have access to an independent and easily-accessible, no-cost dispute resolution service for general grievances originating in a disparate range of personally challenging events. These can include events associated with their working environment, medical treatment, a marital/rela-

tionship dispute, problems with builders working on their home, issues with where or how their neighbours park their car on the street, how their child was dealt with at school following an incident with another child, and so on. However, the DPC, no matter how empathetic it might be to the issues raised, cannot operate beyond its statutory remit. And the risk that arises if both complainants and the DPC over-reach is that data protection regulation as intended is rendered meaningless because it becomes the law of absolutely everything.

An unwelcome trend

Another phenomenon we continued to see in 2020 was that of both organisations and individuals attempting to misuse the GDPR to obfuscate or pursue other agendas. That said, there can be genuine confusion on the part of many as to how GDPR does and does not apply, and sometimes issues are just not black and white. Where inaccurate assertions circulate — whatever the reason or motivation — these will only be resolved over time as we call them out. As an example, an ongoing issue arises with organisations 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.

Breach notifications

The number of breach notifications to the DPC remained high in 2020 but the DPC is more convinced than ever of the value of the mandatory requirement to notify under the GDPR. It allows the DPC to gain insights into the risks around the security and processing of personal data arising in organisations on a case-by-case basis and to intervene and guide on mitigation measures around those risks, where appropriate. In general, the responses we receive from organisations encourage the DPC in the view that most organisations want to comply and value the input of the DPC. Details of breaches notified to the DPC are set out in chapter three.

Special projects relating to Children, Cookies

Special projects undertaken by the DPC in 2020 included the publication of comprehensive draft guidance on the specific protections required for processing children's data under the GDPR which underlines that the best interests of the child must always be to the fore. This draft guidance now open for public consultation is the product of a focussed consultation run by the DPC around the issues of children's data and which involved specific consultation directly with children through their teachers and youth groups. The guidance will benefit children across the EU in particular when implemented by the many platforms operating from Ireland that process the data of EU children. A synopsis of this guidance is set out in chapter eleven of the report.

In addition, the DPC completed early in 2020 a "regulatory sweep" of some of the frequently visited websites in Ireland in order to establish the levels of compliance with

e-privacy regulations (“cookies” regulation) in Ireland. The results of the sweep which were published in April 2020 made for disappointing reading. Following the completion of the exercise, the DPC produced specific and detailed guidance of what is necessary to comply with the regulations. By year-end the DPC had also investigated and commenced enforcement action against a number of website operators. This process of cookies investigations followed by enforcement action will continue throughout 2021. It’s worth equally commenting that the EU Commission has proposed a range of new legislative measures to regulate digital services in the form of the Digital Services Act and the Digital Markets Act. Whatever the final form these laws take, it appears as a positive to the DPC that regulation in this area is being looked at more broadly.

Guidance

The DPC continued its focus on issuing guidance useful to individuals and controllers. In particular, the DPC has also sought in 2020 to increase the supports it provides to the over 2000 Data Protection Officers (DPO) now appointed in organisations across Ireland. The DPO role is a challenging one demanding a range of hard and soft skills. Data protection is a rapidly evolving and advancing area of law and requires specific resources and abilities. The DPC will continue to populate the dedicated area on its website for DPOs and is keen to see skill and resourcing levels rise in this area as responsibility and accountability under GDPR necessarily rest with the data controller in the first instance. Whilst ex-post enforcement by the DPC will always play a central role in the discharge of its regulatory functions, the DPC is also mindful of the importance of encouraging compliance at source.

This importance of encouraging compliance from the outset was well underlined through the intervention by DPC, partly delivered by means of an on-site inspection at Facebook’s premises in Dublin, in February 2020. The DPC had received short notice from Facebook that it planned to roll out a dating service for EU users from mid-February. The DPC sought documentation including the DPIA underpinning the decision to implement this service (and at such short notice) in the EU during its onsite inspection. Arising from this exercise, Facebook deferred implementation, pending resolution of a number of personal data processing issues pertaining to the service. While the newspaper headlines ran to the effect that DPC had “cancelled St Valentine’s Day”, the outcome was positive in terms of ensuring what was rolled out many months later had improved the position of data subjects.

In addition, the DPC continued its commitment to outreach and again spoke at a vast array of events nationally and internationally in order to share information, promote understanding, and debate and clarify its interpretation of the law. The feedback we receive is that these contributions by the DPC are very much appreciated and energise the sectoral groups we address in their efforts to comply.

The Global Pandemic

There’s probably no foreword to any 2020 annual report that can be written without mention of the global pandemic that hit in 2020. For the part of the DPC, the pandemic provided some instructive and clear examples of the true value of the protective framework the GDPR represents. In the many mandatory consultations by Government with the DPC on new public health initiatives with personal data processing implications, the GDPR provided the guard-rails to ensure initiatives were proportionate and secure in terms of how rights of individuals were protected and balanced. The significant consultation and engagement between the DPC and public health authorities on the Covid-19 contact-tracing app provided one obvious example of this. The DPC was particularly pleased to see health authorities in Ireland show leadership — and demonstrate best practice — by publishing the Data Protection Impact Assessment and Source Code for the contact tracing app, helping to ensure a high level of trust amongst the public. Challenging issues around how Covid-19 PCR test results were communicated in certain workplace settings where mass testing was implemented also arose and the GDPR again underpinned the identification of the correct approach, and the balancing of interests required.

Data Transfers, Litigation

In July 2020, the Court of Justice of the European Union delivered judgment in proceedings initiated by the DPC in the Irish High Court in 2016, where the DPC sought a reference on issues relating to the use of Standard Contractual Clauses to underpin personal data transfers from the EU to the US. The CJEU judgment set out a detailed ruling in relation to US laws and practices as they impact on the protection of EU personal data and clarified that regardless of what legal transfer mechanism is used to transfer data, EU users’ personal data must have equivalent protections to that which it enjoys in the EU. The DPC initiated an inquiry into Facebook’s transfers to the US following on from the judgment. This inquiry was the subject of a judicial review by Facebook, which was heard before the High Court in December 2020. Judgment is awaited.

2020 was a busy year overall for litigation for the DPC and a full outline of the cases in which DPC was a party and which concluded or judgment was delivered are set out on page 54. Details of the direct marketing prosecutions of organisations by the DPC which concluded during 2020 can be found in Appendix 3.

EU Cooperation

The DPC’s participation at the European Data Protection Board remained intense in 2020 but logistically easier. Resulting from travel restrictions, all meetings from April onwards were held virtually and in total the DPC contributed to almost 200 meetings of EDPB (between plenary and expert groups) last year, including acting as rapporteur on some files. The goals of harmonisation and democratic input in decision-making are an important

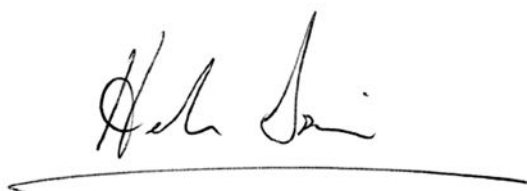
part of the regulatory regime introduced by the GDPR but their implementation in practice remains very much a work in progress.

Brexit

Preparing for the final exit of the UK from the EU continued as a focus for the DPC in terms of ensuring Irish-based organisations understand the data protection implications of the UK becoming a “third country”. The EU-Commission’s short-term (and temporary) initiative to provide for continued data free flows between the EU and UK at the start of 2021 has eased the pressure on Irish organisations for the moment. The EU Commission has announced it will propose an adequacy decision in respect of the UK in the next few months which will require approval through the EU comitology process.

Finally....

The progress the DPC has made in 2020 provides a solid platform on which to build in 2021 across our enforcement and complaint-handling functions in particular. There are many other areas of the GDPR that remain for exploration to the benefit of organisations and data subjects alike including codes of conduct and certification. The GDPR must be understood as a project for the now but equally for the longer-term. The DPC intends to continue as a leader in its full implementation.



Helen Dixon

Commissioner for Data Protection





Executive Summary

Supporting Individuals

From 1 January 2020 to 31 December 2020:

- The DPC received in excess of **23,200** electronic contacts, almost **10,000** phone calls and **2,000** postal contacts;
- The DPC handled a total of **10,151** cases in 2020, up 9% on 2019 figures (9,337).
- The DPC received **4,660** complaints from individuals under the GDPR;
- Overall, the DPC concluded **4,476** complaints, including **1,660** complaints received prior to 2020;
- Over **60%** (2,186) of complaints lodged with the DPC in 2020 were concluded within the same calendar year; and
- The DPC continued to reduce conclusion times for cases (average days taken to conclude a case has reduced by **53%** since the GDPR came into application).

In 2020, the most frequent GDPR topics for queries and complaints continued to be: Access Requests; Fair-processing; Disclosure; Direct Marketing and Right to be Forgotten (delisting and/or removal requests).

10,000
telephone
calls

23,200
emails

2,000
by post

¹ Electronic communications comprise both emails to the DPC's info@ account and webforms submitted

Supporting Compliance

- Total valid breach notifications received in 2020 was **6,628**.
- Breach notifications up **10%** on 2019 figures.
- Of the total recorded breach cases, **90% were concluded** in 2020 (**5,932 cases**).

The most frequent cause of breaches reported to the DPC was unauthorised disclosure (**86%**).

The DPC launched a **redesigned website** in November 2020, making its resources more convenient for users and introducing a new section specifically for DPOs.

In the last year, the DPC has published almost **40 pieces of guidance**, including blogs and podcasts, to make information as accessible as possible for people.

In 2020, the DPC continued to develop its **DPO Network**, transitioning to online supports as a result of the pandemic. In addition to increased resources on its website, DPC staff presented at multiple webinars and events aimed at DPOs.

The DPC continued its partnership with the Croatian Data Protection Authority, AZOP, and Vrije University in Brussels on an EU-Funded project (**The ARC Project**) to provide practical supports to SMEs.

Regulating

As of 31 December 2020, the DPC had **83 Statutory Inquiries** on-hand, including 27 Cross-Border Inquiries.

In May 2020 the DPC issued its first **finer** under the GDPR, levying two separate fines against an Irish state agency.

In the same month, the DPC sent Europe's first major-scale **Article 60 Draft Decision** to the Concerned Supervisory Authorities.

The DPC triggered the EDPB's Article 65 Complaint Resolution Mechanism in 2020, becoming the first supervisory authority to do so.

In December 2020, the DPC issued its **first fine in a cross-border case**, fining Twitter International Company €450,000.

Also in December 2020, the DPC sent forward its second major-scale Article 60 Draft Decision to Concerned Supervisory Authorities. This Draft Decision concerned WhatsApp and was ongoing at year-end.

In 2020 there were **14 judgments** delivered and/or final orders made in proceedings to which the DPC was a party.

Through **Supervision** action, the DPC has brought about the postponement or revision of three scheduled big tech projects with implications for the rights and freedoms of individuals.



6,628
valid data security
breaches
recorded



83
Statutory
Inquiries



**Europe's
First**
major-scale Article
60 Draft Decision
(sent by DPC
May 2020)

Decisions

Some highlighted Decisions from 2020:

Organisations	Decision Issued
Kerry County Council	25-Mar-20
Waterford City and County Council	21-Oct-20
Tusla Child and Family Agency (3 breaches)	07-Apr-20
Tusla Child and Family Agency (1 breach)	21-May-20
Tusla Child and Family Agency (71 breaches)	12-Aug-20
Health Service Executive (HSE South)	18-Aug-20
Health Service Executive (Our Lady of Lourdes Hospital)	29-Sep-20
Ryanair	11-Nov-20
Twitter International Company	9-Dec-20
Groupon	16-Dec-20
University College Dublin	17-Dec-20

Engaging with Civil Society

In 2020, the DPC opened an extensive consultation on its draft guidance on the rights of children as data subjects — ***Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing***. This consultation was still open at year-end.

Engaging with Peers

Since 1 January 2020, the DPC:

- Received **354** complaints from peer Data Protection Authorities (DPAs) in which the DPC was identified as Lead Supervisory Authority;
- Attended over **180** EDPB meetings, most of which were conducted virtually due to pandemic-related travel restrictions;
- Continued to have representatives on all European Data Protection Board (EDPB) subgroups and act as co-coordinator of the Social Media Subgroup; and
- Hosted a virtual meeting of the British, Irish and Islands' Data Protection Authorities (BIIDPA) welcoming representatives from Bermuda, the Cayman Islands, Gibraltar, Guernsey, the Isle of Man, Jersey, Malta and the United Kingdom.

Mainstreaming Data Protection

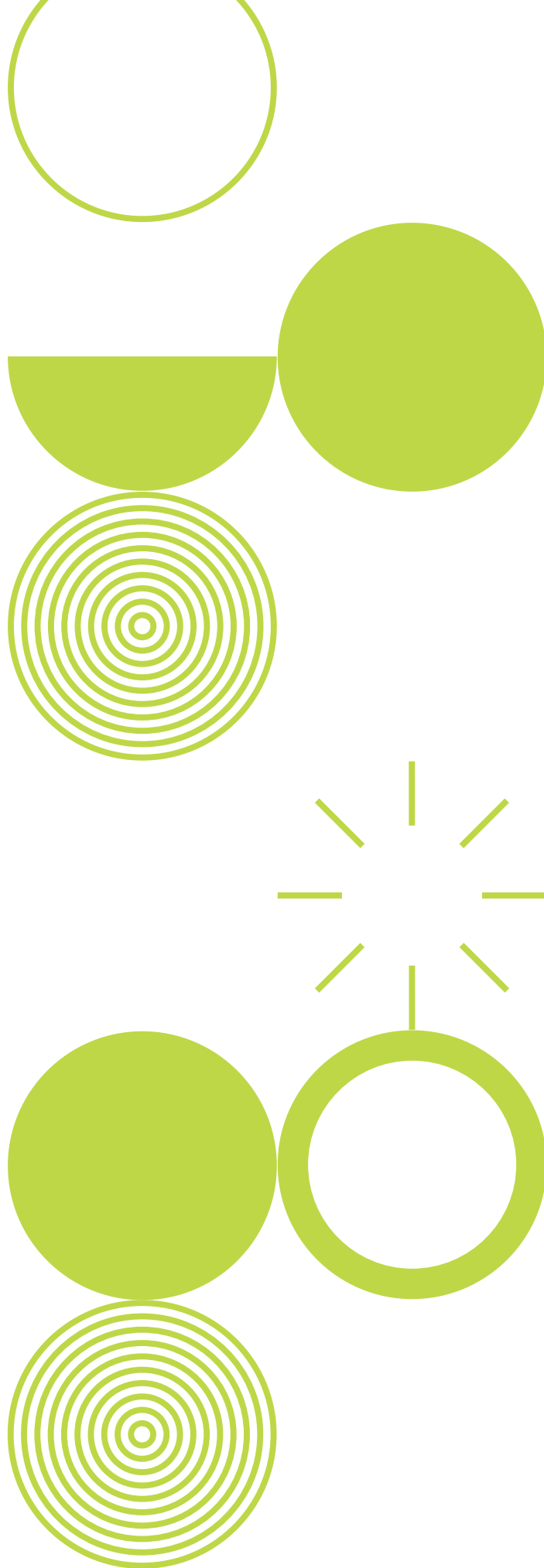
Staff of the DPC presented at almost 100 speaking events in 2020. Since Covid-restrictions came into effect, all staff-participation has been conducted online.

The DPC remains committed to driving awareness of data protection rights and responsibilities, producing almost 40 items of guidance, including technological advice, Cookie compliance and Covid-related concerns.

Other Activity

In 2020 the DPC:

- Concluded **147 electronic direct marketing investigations**;
- **Prosecuted six companies** for sending unsolicited text messages or electronic mail to individuals;
- Handled **37 Law Enforcement Directive complaints**; and
- Increased DPO-registration compliance to **96%** for Public Sector bodies; and
- In April, the DPC published new guidance in relation to the use of cookies and tracking technologies.



1

Roles and Responsibilities

Functions of the DPC

The Data Protection Commission (DPC) is the national independent authority in Ireland responsible for upholding the fundamental right of EU persons to have their personal data protected. Accordingly, the DPC is the Irish supervisory authority tasked with monitoring the application of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

The core functions of the DPC, under the GDPR and the Data Protection Act 2018 — which gives further effect to the GDPR in Ireland — include:

- driving improved compliance with data protection legislation by controllers and processors;
- handling complaints from individuals in relation to potential infringements of their data protection rights;
- conducting inquiries and investigations into potential infringements of data protection legislation;
- promoting awareness among organisations and the public of the risks, rules, safeguards and rights incumbent in the processing of personal data; and
- co-operating with data protection authorities in other EU member states on issues, involving cross-border processing.

The DPC also acts as supervisory authority for personal-data processing under several additional legal frameworks. These include the **Law Enforcement Directive** (Directive 2016/680, as transposed in Ireland under the **Data Protection Act 2018**) which applies to the processing of personal data by bodies with law-enforcement functions in the context of the prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties. The DPC also performs certain supervisory and enforcement functions in relation to the processing of personal data in the context of electronic communications under the **e-Privacy Regulations** (S.I. No. 336 of 2011).

In addition to its functions under the GDPR, the DPC continues to perform its regulatory functions under the **Data Protection Acts 1988 and 2003**, in respect of complaints and investigations that relate to the period before 25 May 2018, as well as in relation to certain limited other categories of processing, irrespective of whether that processing occurred before or after 25 May 2018.

In addition to specific data protection legislation, there are in the region of 20 more pieces of legislation, spanning a variety of sectoral areas, concerning the processing of personal data, where the DPC must perform a particular supervisory function assigned to it under that legislation.

DPC's Senior Team

The DPC's Senior Management Committee (SMC) comprises the Commissioner for Data Protection and the seven Deputy Commissioners. The Commissioner and members of the SMC oversee the proper management and governance of the organisation, in line with the principles set out in the Code of Practice for the Governance of State Bodies (2016). The SMC has a formal schedule of matters for consideration and decision, as appropriate, to ensure effective oversight and control of the organisation.

The DPC's SMC comprises:



Helen Dixon
Commissioner for Data
Protection



Anna Morgan
Deputy Commissioner —
Head of Legal



Colum Walsh
Deputy Commissioner —
Head of Regulatory Activity



Dale Sunderland
Deputy Commissioner —
Head of Regulatory Activity



Graham Doyle
Deputy Commissioner —
Head of Corporate Affairs,
Media & Communications



John O'Dwyer
Deputy Commissioner —
Head of Regulatory Activity



Tony Delaney
Deputy Commissioner —
Head of Regulatory Activity



Ultan O'Carroll
Deputy Commissioner
(Acting) — Head of
Technology & Operational
Performance

Funding and Administration — Vote 44

The DPC is funded entirely by the Exchequer. From 1 January 2020, the DPC was funded through a new Vote of the Oireachtas — Vote 44. The Commissioner for Data Protection is the Accounting Officer for the Commission's Vote. As a Vote body, the Accounting Officer must prepare the Appropriation Account for the DPC's Vote for submission to the Comptroller and Auditor General. As required, this includes the Accounting Officer's statement on the DPC's systems of internal financial control. The 2020 gross estimate provision for Vote 44 — Data Protection Commission was **€16.916M** of which **€10.552m** was allocated for pay-related expenditure, and **€6.364m** of which was allocated to non-pay expenditure. The funding for 2020 represented an **increase of €1.6M** on the 2019 allocation.

The DPC is preparing its financial statement for 2020 and this statement will be published on the DPC's website following the conduct of an audit by the Comptroller and Auditor General.



2

Contacts, Queries and Complaints

Contacts

Stakeholders contact the DPC in a variety of ways, including the DPC Helpdesk, online webforms, email and post. In 2020, the DPC received 23,226 electronic contacts,² 9,410 phone calls³ and 1,881 postal contacts.

2020 presented unique challenges in terms of front-line service provision, including technical and logistical challenges incurred as a result of remote-working requirements. Despite these challenges, service provision was maintained throughout the year. No negative effect on response times or service levels was incurred as a result of remote working, and engagement was commensurate with pre-Covid rates.

² Electronic communications comprise both emails to the DPC's info@ account and webforms submitted through the DPC web-site.

³ The number of phone contacts to the DPC was down in 2020, when compared to previous years. This is accounted for by the transition to remote working (Covid-19) and resulting diminished capacity to process calls (working via mobile phone). Full phone capacity was subsequently restored, once the DPC secured appropriate off-site call services and equipment.

New in 2020 were the significant number Covid-19 related queries the DPC received from individuals and organisations seeking to understand the interplay between data protection law and Covid-19 requirements. In many instances these queries were time sensitive in nature, and necessitated rapid turnaround.

Complaints

The DPC processes complaints under two main legal frameworks:

- Complaints received from 25 May 2018 onwards (and which relate to matters which occurred on or after 25 May 2018) are dealt with under the GDPR, Law Enforcement Directive, and the Data Protection Act 2018; and
- Complaints and infringements occurring before 25 May 2018 are dealt with under the Data Protection Acts 1988 and 2003, even where they are notified to the DPC on or after 25 May 2018.

To constitute a complaint — and therefore trigger the DPC's statutory complaint-handling obligations — the matter must fall under one of the following headings:

- A complaint from an individual relating to the processing of their own personal data;
- A legally authorised person or entity complaining *on behalf of an individual* (e.g. a solicitor on behalf of a client or a parent/ guardian on behalf of their child); or
- Advocacy groups which meet the requirements to act *on behalf of one or more individuals* under the GDPR, LED and the Data Protection Act 2018.

Between 1 January 2020 and 31 December 2020:

- The DPC received 4,660 complaints from individuals under the GDPR and 59 complaints under the Data Protection Acts 1988 and 2003.
- Overall, the DPC concluded 4,476 complaints, including 1,660 complaints received prior to 2020.
- Over 60% (2,186) of complaints lodged with the DPC in 2020 were concluded within the same calendar year.

Complaints Received under the GDPR — Top 5 Issues in 2020

Categories of Complaints	No	% of total
Access Request	1683	27%
Fair Processing	1623	26%
Disclosure	793	12%
Direct Marketing	429	7%
Right to erasure	423	7%

Complaints Received under the Data Protection Acts 1988 and 2003 — Top Five Issues in 2020

Categories of Complaints	No	% of total
Disclosure	24	41%
Fair Processing	14	24%
Access Request	10	17%
Right to be forgotten	4	7%
Security	2	3%

The majority of cases concluded by the DPC in 2020 involved **Access Requests (30%)**. The next highest category of cases concluded involved **Fair Processing (19%)**, followed by **Disclosure (15%)**.

Complaint Handling

Where possible, the DPC endeavours to resolve complaints amicably — as provided for in Section 109(2) of the Data Protection Act 2018. The option to have their issue dealt with by amicable means is afforded to individuals throughout the lifetime of their complaint, regardless of how far the issue may have progressed through escalated channels. Case studies illustrating these escalated channels in operation can be found at the end of this chapter.

Where amicable and early resolution is not possible, the DPC escalates issues according to complaint category:

Access Rights Complaints

Article 15 of the GDPR provides that an individual may obtain from a data controller confirmation of whether or not personal data concerning them are being processed and, where that is the case, access to a copy of that personal. This is an important right and one which gives rise to the largest number of complaints to the Data Protection Commission DPC annually.

The right of access enables an individual to verify the lawfulness of the processing undertaken by the data controller and obtain copies of their personal data for their own records. It is one of the fundamental rights conferred on an individual by the GDPR. It is also a right contained in the Charter of Fundamental rights of the European Union. That said, an individual's right of access is not absolute and may be subject to certain restrictions, including but not limited to those set out at Sections 60 of the Data Protection Act 2018.

The GDPR prescribes a mechanism in Article 23 to permit the restrictions of rights in particular and specific circumstances. Each Member State is permitted to introduce their own exemptions in national legislation. Such restrictions must respect the essence of the fundamental rights and freedoms and must be a necessary and a proportionate measure in a democratic society. In Ireland this has been transduced through Section 60 of the Data Protection Act 2018.

In any examination of complaints undertaken by the DPC, much of the work focuses on an examination of the validity of the exemptions advanced by the data controller in justifying its refusal to provide personal data in response to an access request. In the examination of complaints, the DPC will determine whether or not the data controller has acted appropriately in responding to the access request, which will in most cases involve an examination of how the data controller interpreted the restrictions in the context of the particular circumstances of the case. This may result in additional personal data being released to the data subject.

By way of example, data controllers frequently assert legal privilege over documents containing personal data, as a justification for withholding personal data in response to an access request.

Section 162 of the Data Protection Act 2018 specifically deals with legal professional privilege (LLP). In addition, Section 60(3)(a)(iv) provides that the rights and obligations provided for in Articles 15 are restricted to the extent that data is processed in contemplation of, or for the establishment, exercise or defence of, a legal claim, prospective legal claim, legal proceedings or prospective legal proceedings — whether before a court, statutory tribunal, statutory body or administrative or out-of-court procedure. In both sections the underlining principles are the same and require an evaluation of privilege by the DPC.

When a data controller receives an access request it is required to comply with it without undue delay and at the latest within one month of receipt. In line with the risk-based approach to data protection, which is central to the GDPR, each individual data controller and data processor is required to put in place appropriate technical and organisational measures to ensure and demonstrate that the data processing undertaken complies with legislation. Accordingly a clear organisational policy on to how to action a subject access is prudent, and key to avoiding costly and time consuming repetition of work for organisations.

Legal Privilege and the Right of Access

There are essentially two classes of legal professional privilege- legal advice privilege or litigation privilege. As a first step it is necessary for the DPC to establish the nature of privilege advanced by the data controller.

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. Where the dominant purpose of the communication is to prepare for “actual or apprehended” litigation, litigation privilege may be claimed.

Having established the category of privilege, the next step for the DPC is to assess the privilege status of the personal data. The question as to whether personal data contained in documents are ones to which privilege applies, is essentially a legal question and it is fair to say that the Oireachtas incorporated the common law principles as they apply to privilege in the Data Protection Act 2018.

In any examination of this nature the DPC will require considerable information, including an explanation as to the basis upon which the data controller, is asserting privilege so that we can properly evaluate the validity of reliance on Section 162. Essentially the DPC will seek a narrative of each document containing personal data. In relation to litigation privilege the primary focus when assessing personal data is when litigation came into the minds of the parties, i.e. when it was threatened or contemplated.

Electronic Direct Marketing Complaints

The DPC actively investigates and prosecutes offences relating to electronic direct marketing under S.I.

336/2011 — European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (‘the ePrivacy Regulations’). The ePrivacy Regulations implement Directive 2002/58/EC (‘the ePrivacy Directive’) in Irish law.

The DPC received 144 new complaints in relation to electronic direct marketing in 2020. These included some 66 complaints in relation to email messages, 73 complaints in relation to text messages, and five complaints concerning phone calls. A total of 149 electronic direct marketing investigations were concluded in 2020. This figure comprises one complaint from 2018, 51 from 2019 and 97 from 2020. The DPC prosecuted 6 companies during 2020 for direct marketing infringements, the details of which are set out in Appendix 3.

One-Stop-Shop Complaints

The One-Stop-Shop mechanism (OSS) was established under the GDPR with the objective of streamlining how organisations that do business in more than one EU member state engage with data protection authorities (called ‘supervisory authorities’ under the GDPR). The OSS requires that these organisations are subject to regulatory oversight by just one DPA, where they have a ‘main establishment’, rather than being subject to regulation by the data protection authorities of each member state. The main establishment of an organisation is generally its place of central administration and/or decision making. In the case of a data processor that has no place of central administration, then its main establishment will be where its main processing activities in the EU take place.

In 2020, the DPC received **354 cross-border processing complaints** through the OSS mechanism that were lodged by individuals with other EU data protection authorities.

Data-Breach Complaints

The DPC also handles complaints relating to both notified and non-notified data breaches. The majority of data-breach complaints arise as a result of a notification to the DPC — from an organisation or entity — that there has been a breach in relation to the personal data for which they are the data controller. Data-breach complaints may also arise in circumstances where an individual has become independently aware of a data breach, often through media coverage, or through adverse impact arising from the breach (e.g. unauthorised access to email accounts, customer or bank accounts, etc.).

Law Enforcement Directive Complaints

The EU Directive known as the Law Enforcement Directive (EU 2016/680) (the LED) was transposed into Irish law on 25 May 2018 with the enactment of the Data Protection Act 2018. The LED applies where the processing of personal data is carried out for the purposes of the

prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties. In order for the LED to be applicable, the data controller must also be a “competent authority” as set out in Section 69 of the Data Protection Act 2018.

In 2020, the DPC handled 37 LED complaints, in the majority of which the Irish police force, An Garda Síochána (AGS), were the data controller. Complaints also included organisations such as the Irish Prison Service, the Revenue Commissioners, the Department of Agriculture & Food, as well as several local authorities.

Section 91 of the Data Protection Act 2018 applies to the processing of personal data for law enforcement purposes and sets out the conditions for individuals to access, rectify or erase their personal data. Requests to access a copy of data recorded on AGS systems, details of a prosecution by the Revenue Commissioners against a person, or a litter fine imposed by a local authority are referred to as Section 91 LED subject access requests.

The DPC frequently encounters cases where data subjects make subject access requests seeking third party information such as the name and address of the perpetrator of an alleged assault, or the details of a person who reported a matter in confidence. Section 91(7) of the Data Protection Act 2018 provides that a data controller (competent authority under the LED) shall not provide individuals with personal data relating to another individual where doing so would reveal, or would be capable of revealing, the identity of the other individual. The only circumstances in which 91(7) does not apply is where a third party consents to the provision of their information to the data subject making the request as set out in 91(8) of the Act. Section 91(9) of the Act also provides that the right of access shall not apply to data that consists of an expression of an opinion about an individual by another person given in confidence or on the understanding that it would be treated as confidential.

Complaints received under the Data Protection Acts 1988 and 2003

The DPC continues to receive and examine complaints that fall under the Data Protection Acts 1988 and 2003. Under both the 2018 Act and the 1988 and 2003 Acts, it is the statutory obligation of the DPC to strive to amicably resolve complaints that are received from members of the public. In 2020, the vast majority of complaints falling under the 1988 and 2003 Acts were concluded amicably between the parties to the complaint, without the necessity for issuing a formal decision under Section 10 of the 1988 and 2003 Acts. The Commissioner has issued 77 formal decisions under the Data Protection Acts 1988 and 2003 since January 2020 of which 50 fully upheld the complaint and 18 rejected the complaint. In a further nine instances, the complaint was partially upheld.

Complaints concluded with Decisions under the Data Protection Acts 1988 and 2003

Complaint upheld	50
Complaint rejected	18
Complaint partially upheld	9
Total:	77

Data protection and the courts when acting in their judicial capacity

Although the DPC is the supervisory authority for data protection laws in Ireland, special rules apply where the courts are engaging in processing activities. These special rules come from Article 55(3) of the GDPR, which prohibits the DPC, like other EU DPAs from supervising the data processing operations of the courts when they are acting in their judicial capacity. This is to ensure the independence of the judiciary in the performance of its judicial tasks, including decision-making.

Sections 157 to 160 of the Data Protection Act 2018 along with the relevant Rules of Court regulate how the Irish courts must process personal data and how certain data protection rules in the GDPR should be given effect (including any restrictions on data protection rights). This includes a provision for the assignment of a specific judge by the Chief Justice of Ireland to act as the data protection supervisor in relation to the processing of personal data, which occurs when the Irish courts are acting in their judicial capacity. More information on the supervision of data processing by the Irish courts when acting in their judicial capacity can be found at <https://www.courts.ie/courts-data-protection-notice>

Distinguishing the roles of the DPC and Assigned Judge

Not all processing activities connected with the courts will necessarily come within the scope of the courts acting in their judicial capacity. For data protection matters that fall outside of that scope, the DPC will be the relevant supervisory authority. The DPC receives complaints from individuals where the issues raised may in fact relate to the courts acting in their judicial capacity and therefore are not matters that the DPC can handle. Other complaints relating to broader court activities come with the DPC's remit.

The following examples illustrate the areas where the DPC or the Assigned Judge is the appropriate supervisory authority.

Example A:

The Courts as an employer

(Cases where the DPC is the competent supervisory authority)

The Court Service admitted that a manager used CCTV to monitor an employee's working hours.

As the matters complained of do not come within the data processing activities of the courts acting in their judicial capacity, the DPC was the appropriate authority to deal with this complaint.

Example B:

Disclosure of Court Orders held by third parties

(Cases where the DPC is the competent supervisory authority)

The complainant was party to Family Law proceedings in which the District Court Judge directed that the children of the parties be referred for play therapy. The solicitors for the mother disclosed two court orders (relating to access) to the play therapist. This was in the absence of a court order to do so or at the request of the play therapist. The information contained in the orders was not necessary for the purposes of the play therapy and disclosed information relating to other matters including maintenance.

As the matters complained of do not come within the data processing activities of the courts acting in their judicial capacity, the DPC was the appropriate authority to deal with this complaint.

Example C:

Disclosure of personal data on a voluntary basis

(Cases where the DPC is the competent supervisory authority)

The complainant's personal data was included in a voluntary Affidavit of Discovery sworn by a non-party to the proceedings. This happened in the absence of a Court Order compelling non-party discovery and therefore there was no legal basis to make the discovery.

As the matters complained of do not come within the data processing activities of the courts acting in their judicial capacity, the DPC was the appropriate authority to deal with this complaint.

Example D:

Access to the Court file

(Cases where the Assigned Judge is the competent supervisory authority)

The complainant made an access request to a local court office for all personal data held by the Courts Service relating to him arising from an appearance before the court, including the court records and the digital audio recording of the hearing. The request was refused.

As the matters complained of come within the data processing activities of the courts acting in their judicial capacity, the Assigned Judge was the appropriate authority to deal with this complaint.

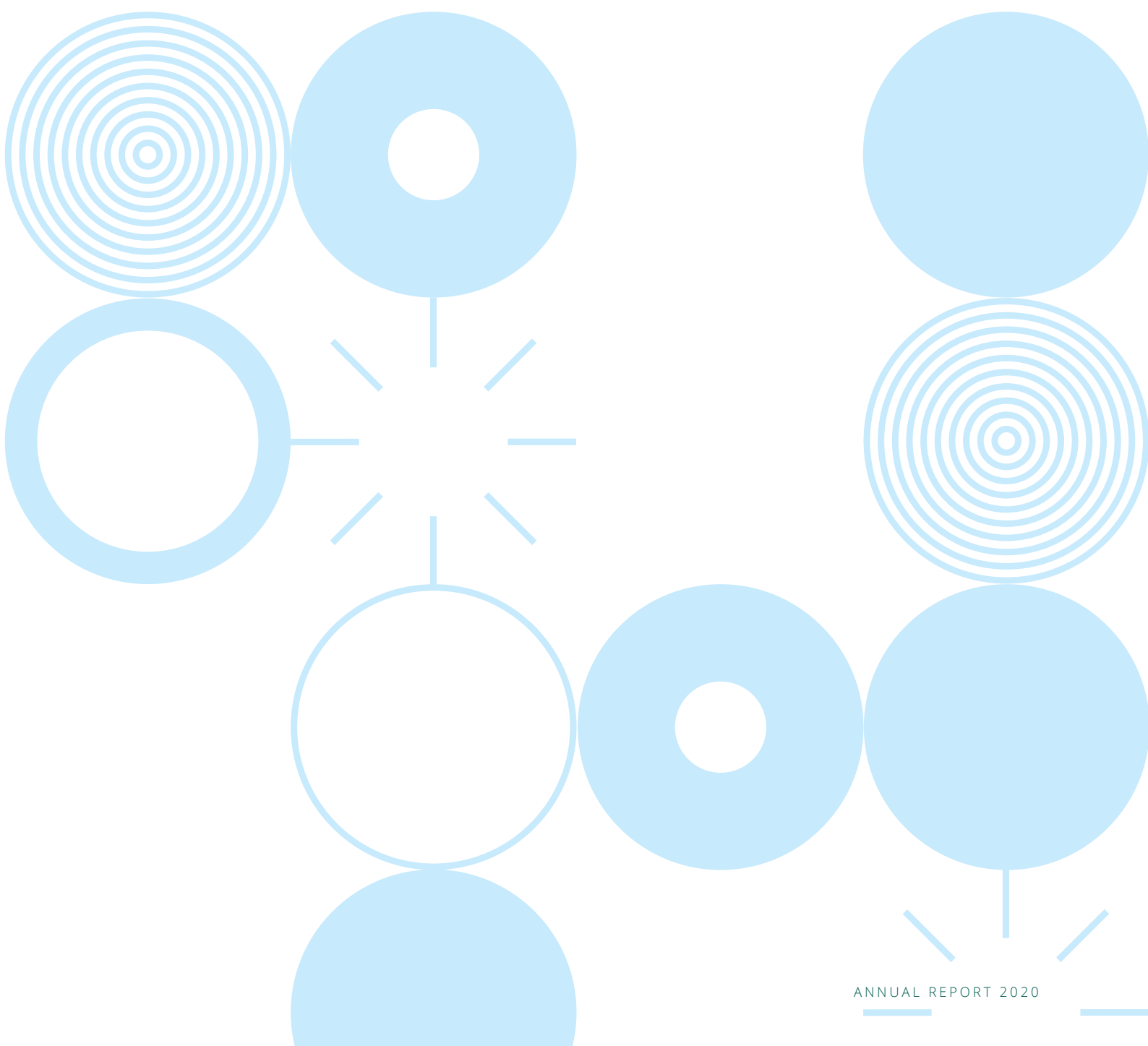
Example E:

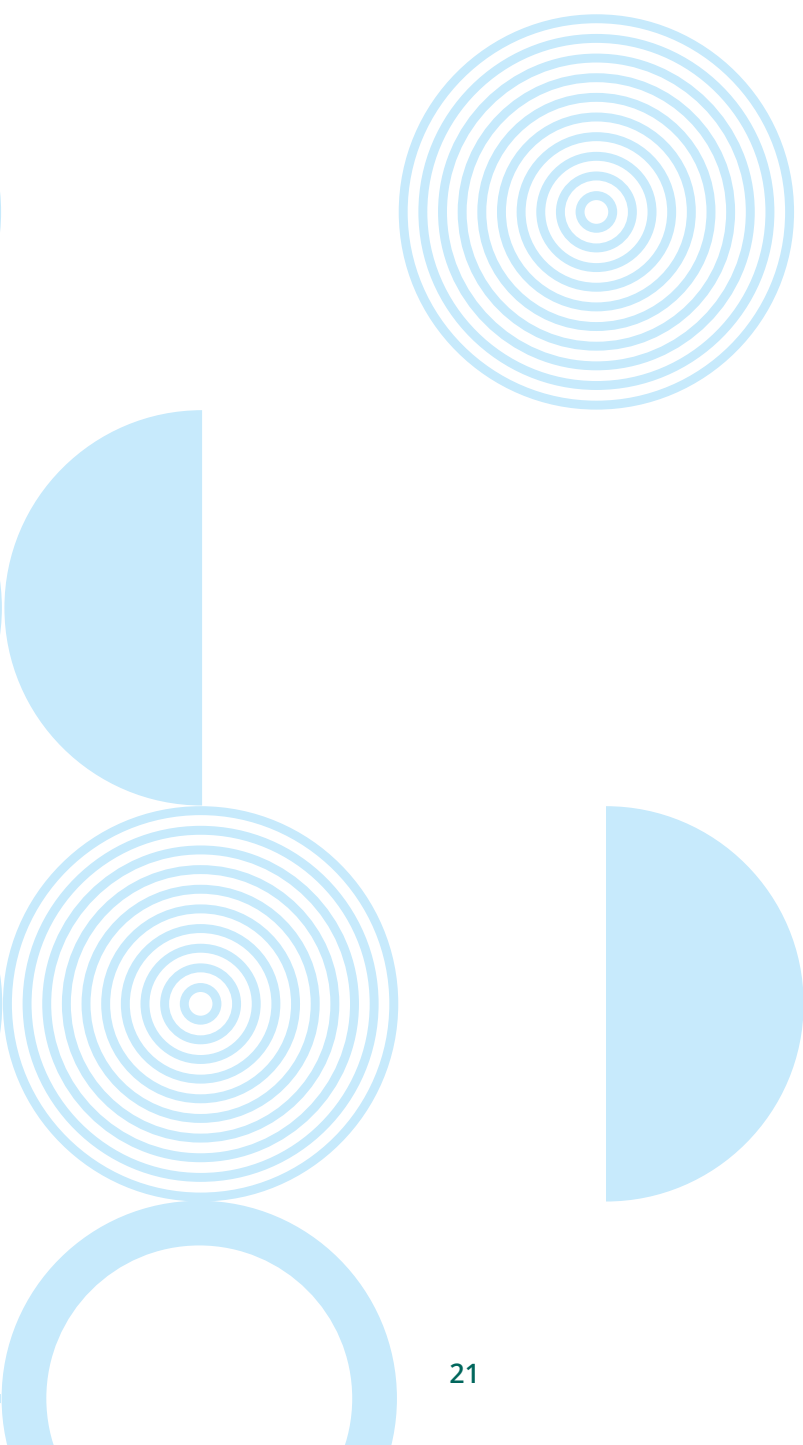
Complaints about the Court Record

(Cases where the Assigned Judge is the competent supervisory authority)

The complainant (who was the defendant in proceedings before the courts) alleges irregularities in the orders made by the court and sought rectification of these.

As the matters complained of come within the data processing activities of the courts acting in their judicial capacity, the Assigned Judge was the appropriate authority to deal with this complaint.





Case Studies

Case Study 1:

Unauthorised publication of a photograph (Amicable Resolution)

The DPC received a complaint from an individual regarding the publication of their photograph in an article contained in a workplace newsletter without their consent. The data controller, who was the individual's public sector employer, informed the individual that it should have obtained consent to use the photograph in the workplace newsletter as this was not the purpose for which the photograph was obtained. The data controller also informed the individual that a data breach had occurred in this instance.

This complaint was identified as potentially being amicably resolved under Section 109 of the Data Protection Act 2018, with both the complainant and data controller agreeing to work with the DPC to try to amicably resolve the issue.

The data controller engaged with the DPC on the matter, and advised that it had conducted an internal investigation and determined that a data breach did occur and that consent should have been obtained to use the individual's photograph in the workplace newsletter. The purpose(s) for which the photograph was initially obtained did not include publication in a newsletter. An apology from the employer was issued to the individual. However, the complainant did not deem this to be an appropriate resolution to the complaint at hand.

The DPC provided recommendations that a consent information leaflet be distributed to staff in advance of using photography, audio and/or video, and that a consent form for photography, audio and video be completed and signed prior to images or recordings being obtained, which the controller subsequently implemented.

Article 5(1)(b) of the GDPR states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation')

The DPC was satisfied that the data controller further processed the individual's personal data without their consent (or other legal basis) for doing so when it published the employee photograph in the workplace newsletter. The DPC issued an outcome letter advising the complainant of same. The DPC was satisfied with the organisational measures subsequently introduced and as such no further actions by the controller in this case was warranted.

In this case study, the risks to the fundamental rights and freedoms of the individual could not be deemed significant, but nonetheless the personal data processing upset the individual and is an infringement of GDPR in the circumstances. This underlines the need for all organisations to train staff — at all levels and in all roles — to be aware of the GDPR and take account of its principles.

Case Study 2:

No response received to subject access request (Amicable Resolution)

The DPC received a complaint from an individual regarding a subject access request made by them to a data controller, an auction house whose platform the complainant had used to sell goods, for a copy of all information relating them. No response was received from the data controller despite the individual issuing two subsequent reminders.

This complaint was identified as potentially being capable of amicable resolution under Section 109 of the Data Protection Act 2018, with both the complainant and data controller agreeing to work with the DPC to try to amicably resolve the matter.

The data controller engaged with the DPC on the matter and informed us that while it previously had a business relationship with the individual in 2016, it did not hold any information relating to them as it had installed a new system in May 2018, and no data was retained prior to that. It further informed the DPC that it had shredded all paper files and that its legal adviser's informed them it was not a requirement to retain same.

The data controller also provided the DPC with screenshots from its electronic system of the results of a search against the individual's name, which did not identify any results to display.

Article 12(3) of the GDPR states that *"the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request."*

Having examined the matter thoroughly, it was apparent to the DPC that the data controller contravened Article 12(3) of the GDPR as controllers have an obligation to provide a response to the individual's subject access request within the statutory timeframe as set out in Article 12 of the GDPR, even where the controller is not in possession of any such data.

Regarding the individual's subject access request no further action on this matter was warranted as there was no evidence to suggest that any data relating to the individual was held by the data controller.

The DPC issued advice to the data controller, reminding it of its obligations specifically under Articles 12 and 15 and the requirement to provide information on actions taken in relation to a subject access request, even in circumstances where this is to inform an individual that it does not hold any data.

Case Study 3:

Retention of a minor's personal data by a State Agency (Amicable Resolution)

(Applicable Law — Data Protection Acts, 1988 and 2003)

In this case, the complainants involved had previously requested that an Irish state agency erase a file pertaining to an incident at school involving their young child which had originally been notified to the agency. However while the agency had decided that the incident did not warrant further investigation, it had refused to erase the minor's personal data — indicating that such files are retained until the minor in question reaches the age of 25 years.

The DPC requested that the state agency outline its lawful basis for the retention of the minor's personal data. The agency provided this and cited its retention policy as stated to the complainants, but the DPC did not consider a blanket retention period applicable in the particular circumstances.

The DPC informed both parties of the amicable resolution process and both expressed a willingness to engage on same. After iterative engagement between the complainants and the controller to discuss the matter, the state agency confirmed to the complainants that the file containing their child's personal data would be deleted.

Case Study 4:

Legal Privilege invoked to withhold personal data (Access Request Complaints)

The DPC dealt with a case which concerned an application by an individual to a hospital for their personal data. This individual had instructed their solicitor in relation to a negligence action against the hospital arising from care they received.

By the time the individual made a complaint the DPC through their solicitor the hospital had released some medical records, but the individual advised that they were awaiting non-clinical notes which the hospital was refusing to release on the basis that they were subject to litigation privilege. Specifically the individual (who was represented by their solicitor in the complaint to the DPC) was of

the view that various staff statements had been withheld. Through the complaint-handling process the DPC established that staff statements had been prepared in the course of an internal review by the hospital of the care of the patient.

The DPC requested sight — on a voluntary basis — of the documentation withheld from the individual in response to the access request, in order to be satisfied that their contents and eligibility for exemption from release had been validly applied.

In circumstances where the statement 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, the DPC was not satisfied that litigation privilege applied and directed that they be released.

Case Study 5:

Attendance Monitoring and Facial Recognition at a secondary school (Direct Intervention)

Following media reports regarding a facial recognition trial for attendance monitoring purposes in a secondary school, the DPC met with members of staff and the Board of Management of the school in February 2020.

The DPC outlined the data protection issues surrounding the use of biometrics data, specifically facial recognition technology, in an educational environment, including processing the data of minors. The DPC referred to the Swedish data protection authority's first fine under GDPR, concerning a trial project in a secondary school where facial recognition technology was used to register student attendance.

The DPC stepped through the definition of biometric data as set out in Article 4(14) of the GDPR and highlighted additional GDPR provisions in Article

5 — Purpose limitation and data minimisation; Article 9 — Sensitive data; and Articles 35 and 36 — Data Protection Impact Assessment (DPIA) and Prior Consultation.

Subsequent to the meeting, the school provided the DPC with a full written report on the matter, including confirmation that it did not proceed to trial the attendance monitoring product in question.

European data protection authorities have traditionally adopted strong positions with regard to facial recognition in schools and the use of biometric attendance systems in the education sector. In Ireland, the DPC regularly conducts inspections of schools where reports of biometric attendance systems or trials are received. The DPC considers that exposure to intrusive methods of surveillance without sufficient legal basis or justification can desensitise students at a young age to such technology and lead to them ceding their data protection rights in other contexts also.

Case Study 6:

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)

The DPC received a complaint from an Irish individual against Cardmarket, a German e-commerce and trading platform. The individual received an email from Cardmarket, 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.

Under the One-Stop-Shop (OSS) mechanism created by the GDPR, the location of a company's main European establishment dictates which European authority will act as the lead supervisory authority in relation to any complaints received. Once the lead authority (LSA) is established, the authority that received the complaint acts as a concerned supervisory authority (CSA). The CSA is the intermediary between the LSA and the individual. Among other things, the reason for this separation is so that supervisory authorities can communicate with individual complainants in their native language.

In this case, the Berlin DPA acted as the LSA, as the company had its main establishment in the Berlin territorial area. The DPC acted as a 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 Berlin DPA concluded its investigation into the breach and the individual's complaint. It uploaded two draft decisions, one in relation to the overall breach which impacted many other users of the platform throughout Europe, and another in relation to the specific complaint which had been lodged by

the Irish individual with the DPC and communicated to the Berlin DPA.

An important aspect of the OSS mechanism is that a CSA may comment on a draft decision issued by a lead supervisory authority. This is to ensure that European supervisory authorities are applying the GDPR consistently i.e. that a final decision reached by the Berlin DPA would have the same conclusion as a decision of the DPC if the company had been located in Ireland and the DPC had investigated the complaint as the lead supervisory authority.

The DPC were satisfied with the Berlin DPA draft decisions and did not consider it necessary to raise any points of clarification or requests for amendment on this occasion.

The draft decision in relation to the overall breach described a number of measures taken by the platform to address the breach and mitigate its adverse effects. The measures included taking its servers off of their network and deleting all the data on them, as well as resetting all user passwords and ensuring new passwords were encrypted with the latest hashing methods. The draft decision considered that a repetition of the incident was unlikely, and that the mass disclosure of passwords had been rendered practically impossible in light of the measures taken.

The DPC informed the individual of the outcome of the Berlin DPA's investigation, providing them with a copy of the overall decision investigating the breach and the decision dealing with their specific complaint.

This case illustrates the challenging handoffs and handovers involved in the OSS mechanism established by the GDPR. It demonstrates the depth of cooperation between European supervisory authorities required for the consistent application of the GDPR in Europe.

Case Study 7:

The Operation of the Article 60 Procedure in Cross Border Complaints: Groupon

The DPC received a complaint in July 2018 from the Polish data protection authority on behalf of a Polish complainant against Groupon International Limited ("Groupon"). The complaint related to the requirements that Groupon had in place at that time to verify the identity of individuals who made data protection rights requests to it. In this case, the complainant alleged that Groupon's practice of requiring them to verify their identity by way of electronic submission of a copy of a national identity card, in the context of a request they had made for erasure of personal data pursuant to Article 17 of the GDPR, constituted an infringement of the principle of data minimisation as set out in Article 5(1)(c) of the GDPR, in circumstances where there was no requirement to provide an identity document when a Groupon account was created. In addition, the complainant alleged that Groupon's subsequent failure to act on the erasure request (in circumstances where the individual objected to providing a copy of their national identity card) constituted an infringement of their right to erasure under Article 17.

The DPC commenced an examination of the complaint upon receipt of same. In the course of its correspondence with Groupon on the matter, it became clear that Groupon's policy of requiring a requester to provide a copy of a national identity card, which had been in place since before the GDPR came into force (and which was in place at the time of the complainant's erasure request), had been discontinued since October 2018. In its place, Groupon had implemented an email authentication system which allowed Groupon users to verify their account ownership. The DPC attempted to amicably resolve the complaint (pursuant to section 109(2) of the Data Protection Act 2018), but the complainant

was unwilling to accept Groupon's proposals in respect of same. As such, the matter fell to be decided by way of a decision under Article 60 of the GDPR.

(i) Initial Draft Decision

The first step in the Article 60 process entailed the DPC preparing a draft decision in respect of the complaint. In its initial draft decision, the DPC made findings of infringements of Articles 5(1)(c) and 12(2) of the GDPR by Groupon. The DPC provided the draft decision to Groupon to allow it to make submissions. Groupon subsequently provided a number of submissions, which (along with the DPC's analysis thereof) were taken into account in a further version of the draft decision.

(ii) Provision of Initial Draft Decision to Concerned Supervisory Authorities

The second stage in the Article 60 process involved the DPC's initial draft decision being uploaded to the IMI to be circulated amongst the Concerned Supervisory Authorities (CSAs), pursuant to Article 60(3) of the GDPR. The DPC's draft decision was uploaded to the IMI on 25 May 2020 and, pursuant to Article 60(4) of the GDPR, CSAs were thereafter entitled to four weeks in which to submit any relevant and reasoned objections to the decision.

The DPC subsequently received a number of relevant and reasoned objections and comments on its decision from CSAs. In particular, certain CSAs argued that additional infringements of the GDPR ought to have been found, and in addition that a reprimand and/or administrative fine ought to have been imposed.

(iii) Revised Draft Decision

The next stage of the Article 60 process required the DPC to carefully consider each relevant and reasoned objection and comment received in respect of its draft decision, and incorporate its analysis of same into a revised draft decision. In revising its draft decision, the DPC followed certain relevant and reasoned objections received, and declined to follow certain relevant and reasoned objections. The DPC's revised draft decision, taking into account its analysis of the relevant and reasoned objections and comments in respect of its draft decision, found additional infringements of

Articles 17(1)(a) and 6(1) of the GDPR by Groupon. In addition, the DPC proposed in its revised draft decision to issue a reprimand to Groupon, pursuant to Article 58(2)(b) of the GDPR. The DPC provided its revised draft decision to Groupon to allow it to make final submissions. A number of final submissions were received from Groupon, which (along with the DPC's analysis thereof) were taken into account in the DPC's revised draft decision.

(iv) Provision of Revised Draft Decision to Concerned Supervisory Authorities

The next stage of the Article 60 process entailed the DPC uploading its revised draft decision to the IMI, for circulation among the CSAs. Under Article 60(5) of the GDPR, CSAs were entitled to two further weeks in which to indicate if they planned to maintain their objections. This raised the prospect that the Dispute Resolution procedure under Article 65 of the GDPR would have to be engaged, which would have involved the European Data Protection Board (EDPB) adjudicating on the point(s) of disagreement, and which would have extended further the time in which the decision in respect of the case could be completed. However, the additional query was subsequently withdrawn.

(v) Adoption of Final Decision

Upon the withdrawal of the final relevant and reasoned objection, and the passing of the deadline for receipt of any further objections, the last stage of the Article 60 process entailed the DPC adopting the final decision, which was uploaded to the IMI and communicated to Groupon. The final decision

was uploaded on 16 December 2020. As per Article 60(6) of the GDPR, the CSAs were deemed at this point to be in agreement with the decision and to be bound by it. Pursuant to Article 60(7), the Polish data protection authority with which the complaint was initially lodged was responsible for informing the complainant of the decision.

In summary, the DPC found infringements of the following Articles of the GDPR in respect of this case: Articles 5(1)(c), 12(2), 17(1)(a) and 6(1).

This case study demonstrates that, where a cross border data protection complaint cannot be amicably resolved, the Article 60 procedure that follows as a result is particularly involved, complex and time-consuming, especially as the views of other supervisory authorities across the EU/EEA must be taken into account and carefully considered in all such cases. In this case, following the completion of the investigation of the complaint, the initial draft of the DPC's decision was uploaded to the IMI on 25 May 2020, and the final decision — incorporating submissions from Groupon, relevant and reasoned objections and comments from CSAs, and the DPC's analysis thereof — was adopted on 16 December 2020, some seven months later.

Case Study 8:

Amicable Resolution in Cross Border Complaints: MTCH

The DPC received a complaint in June 2020, via its complaint webforms, against MTCH Technology Services Limited (Tinder). Although the complaint was made directly to the DPC, from an Irish resident, upon assessment it was deemed to constitute a cross border complaint because it related to Tinder's general operational policies and, as Tinder is available throughout the EU, the processing complained of was therefore deemed to be of a kind *"...which substantially affects or is likely to substantially affect data subjects in more than one Member State"* (as per the definition of cross border processing under Article 4(23) of the GDPR).

The complaint related to the banning of the complainant from the Tinder platform, subsequent to which the complainant had made a request to Tinder for the erasure of his personal data under Article 17 of the GDPR. In response to his request for erasure, the complainant was referred by Tinder to its privacy policy for information in relation to its retention policies in respect of personal data. In particular, Tinder informed the complainant that "after an account is closed, whatever the reason (deletion by the user, account banned etc.), the user's data is not visible on the service anymore (subject to allowing for a reasonable delay) and the data is disposed on in accordance with [Tinder's] *privacy policy*".

The complainant was dissatisfied with this response and followed up with Tinder again requesting the erasure of his personal data. Tinder responded by reiterating that "...personal data is generally deleted 'upon deletion of the corresponding account', further noting that deletion of such personal data is 'only subject to legitimate and lawful grounds to retain it, including to comply with our statutory data retention obligations and for the establishment, exercise or defence of legal claims, as permitted under Art. 17(3) of GDPR.'" The complainant subsequently made his complaint to the DPC.

Upon the DPC's engagement with Tinder in respect of this complaint, Tinder informed the DPC that the

complainant had been banned from the platform as his login information was tied to another banned profile. Also, Tinder identified eleven other accounts associated with the complainant's device ID. All these accounts had been banned from the Tinder platform as it appeared that an unofficial client was being used to access Tinder (a violation of Tinder's terms of service). The DPC reverted to the complainant with this information, and the complainant advised that he had used the official Tinder client for Android and the official Tinder web site on Firefox. However, it transpired that he had been using a custom Android build on his phone with various security and privacy add-ons. As a result, his phone had a different device ID after each update/reboot. In the complainant's view, this was the likely cause of the issue that resulted in his being banned from Tinder. In light of such a ban, as per Tinder's policy on data retention, his personal data would have been retained for an extended period of time. However, in the circumstances, by way of a proposed amicable resolution, Tinder offered to immediately delete the complainant's personal data so that he could open a new account.

The complainant had certain residual concerns regarding the manner in which Tinder responds to erasure requests. Upon being informed that such matters were being examined by the DPC by way of a separate statutory inquiry, the complainant agreed to accept Tinder's proposal for the amicable resolution of the complaint. As such, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and under section 109(3) of the Act the complaint was deemed to have been withdrawn.

This case study demonstrates that a thorough examination of a seemingly intractable complaint can bring about its amicable resolution, which will often result in a fair and efficacious solution for the affected individual in a timely manner. In this case, the information gleaned by the DPC when it probed in more depth into the circumstances of the complainant's ban from Tinder — namely the fact that the complainant used a custom Android build with security and privacy add-ons — contributed to a greater understanding between the parties and led to Tinder making its proposal for the resolution of the case, which the complainant accepted.

Case Study 9:

Amicable Resolution in Cross Border Complaints: Facebook Ireland

The DPC received a multi-faceted complaint in April 2019 relating to requests for access (under Article 15 of the GDPR), rectification (under Article 16 of the GDPR) and erasure (under Article 17 of the GDPR) that the complainant had made to Facebook Ireland Limited ("Facebook"). The complaint was made directly to the DPC, from a data subject based in the UK. Upon assessment in the DPC, the complaint was deemed to be cross border because it related to Facebook's general operational policies and, as Facebook is available throughout the EU, the processing complained of was therefore deemed to be of a kind *"...which substantially affects or is likely to substantially affect data subjects in more than one Member State"* (as per the definition of cross border processing under Article 4(23) of the GDPR).

The complainant initially made his requests to Facebook because his Facebook account had been locked for over a year, without reason in the view of the complainant, and he believed Facebook held inaccurate personal data relating to him. Wishing to ultimately erase all the personal data that Facebook held in relation to him, the complainant was of the view that this inaccurate information was preventing him from being successfully able to log into his Facebook account to begin the erasure process. He had therefore made an access request to Facebook, but had been unable to verify his identity to Facebook's satisfaction. The complainant subsequently made his complaint to the DPC.

After a considerable amount of engagement by the DPC with both Facebook and the complainant with a view to amicably resolving the complaint, in the course of which the complainant was able to verify his identity to Facebook's satisfaction, Facebook agreed to provide the complainant with a link containing the personal data that it held in relation to him. The complainant accessed the material at the link, but remained dissatisfied because he

claimed that the material provided was insufficient. In particular, the complainant indicated that he wished to be advised of any personal data held in relation to him by Facebook beyond that which was processed in order to operate his Facebook profile.

Facebook responded to the DPC indicating that the material provided to the complainant via the link was the totality of the account data that it held in relation to him. The complainant remained dissatisfied with this response, indicating that he wished to obtain information regarding any personal data that Facebook held in relation to him that was not related to his Facebook account. He also reiterated his belief that some of this personal data, allegedly held by Facebook but not related to his Facebook account, may be inaccurate, in which case he wished to have it rectified.

In response, Facebook advised the DPC that, since the commencement of the complaint, it had made certain enhancements to its 'Download Your Information' tool. Following this update to its access tools, it had determined that a very small amount of additional personal data existed in relation to the complainant's Facebook account, and provided the complainant with a new link containing all of the personal data it held in relation to the complainant, including this additional data. The complainant accessed this additional material and, with a view to resolving his complaint, sought confirmation that, once the deletion of his account was effected, Facebook would no longer hold any personal data in relation to him. Facebook reverted to indicate that the material it had provided to the complainant was the totality of the data it held in relation to him that fell within the scope of Article 15, and indicated that it would proceed with the erasure of the complainant's personal data once he had indicated that he was now satisfied for it to do so.

The complainant was content to conclude the matter on this basis and, as such, the matter was amicably resolved pursuant to section 109(3) of the Data Protection Act 2018 (the Act), and under section 109(3) of the Act the complaint was deemed to have been withdrawn.

This case study demonstrates the benefits — to individual complainants — of the DPC's intervention by way of the amicable resolution process. In this case, the DPC's involvement led to the complainant

being able to verify his identity to Facebook's satisfaction, and to Facebook providing him with links containing his personal data on two occasions. The DPC's engagement with the controller also resulted in it confirming, to the complainant's satisfaction, that all the personal data that fell to be released in response to an Article 15 request had been provided to him. This resulted in a fair outcome that was satisfactory to both parties to the complaint.

This case study also illustrates the intense resource-investment necessary on the part of DPAs to resolve issues of this nature. The complainant in this case raises an issue of concern to themselves and is entitled to have that addressed. The question the case raises is whether the controller in this case should have been capable of resolving this matter without the requirement for extensive DPA-resources to mediate the outcome.

Case Study 10:

Article 60 Non-response to an Access Request by Ryanair

In this case, the complainant initially submitted their complaint to the Information Commissioner's Office (ICO) of the UK, which was thereafter received by the DPC, on 2 March 2019. The complaint related to the alleged failure by the Ryanair DAC (Ryanair) to comply with a subject access request submitted to it by the complainant on 26 September 2018 in accordance with Article 15 of the GDPR. The ICO provided the DPC with a copy of the complaint form submitted to the ICO by the complainant, a copy of the acknowledgement, dated 26 September 2018, that the complainant had received from the data controller when submitting the access request, and a copy of the complainant's follow up email to the data controller requesting an update in relation to their request.

Acting in its capacity as Lead Supervisory Authority, the DPC commenced an examination of the complaint by contacting the data controller, outlining the details of the complaint and instructing the data controller to respond to the access request in full and to provide the DPC with a copy of the cover letter that issued to the complainant. Ryanair provided the complainant with access to copies of their personal data relating to the specific booking reference that the complainant had provided to the ICO and data

relating to a separate complaint. Ryanair advised that it could not provide the complainant with a copy of the call recording they had requested as, due to the delay on Ryanair's part in processing the request, the call recording had been deleted in accordance with company policy and they had been unable to retrieve it. Ryanair advised the DPC that it had previously informed the complainant of this via its online portal. Ryanair stated that at the time the request was submitted, due to the volume of data subjects who did not verify their email address, access requests were not assigned to the relevant department until the email was verified by the data subject. Ryanair advised the DPC that the complainant responded to the request, verifying their email address, but the agent who was working on the request had ceased working on the online portal and therefore the request had not been assigned to the relevant department. Ryanair asserted that this error was not discovered until sometime later, when the request was then assigned to the Customer Services department to provide the necessary data, including the call recording, at which point the call record had been deleted in accordance with Ryanair's retention policy. Ryanair provided the DPC with a copy of its retention policy, in which it states that call recordings are retained for a period of 90 days from the date of the call. Ryanair advised that, as the complainant's call had been made on 5 September 2018, it would have been automatically deleted on 04 December 2018. Ryanair further stated that it does not have the functionality to retrieve deleted call recordings.

Pursuant to Section 109(2) of the Data Protection Act 2018, the DPC attempted to facilitate the amicable resolution of the complaint. However

the complainant was unwilling to accept Ryanair's proposals in respect of same. As such, the matter fell to be decided by way of a decision under Article 60 of the GDPR.

(i) Initial Draft Decision

As the complaint related to cross border processing, the DPC was obliged, in accordance with the Article 60 process, to make a draft decision in respect of the complaint. In its initial version of the draft decision, the DPC made a finding of infringement of Article 15 of the GDPR in that Ryanair failed to provide the complainant with a copy their personal data that was undergoing processing at the time of the request. The DPC also found an infringement of Article 12(3) of the GDPR in that Ryanair failed to provide the complainant information on action taken on their request under Article 15 within the statutory timeframe of one month. The DPC provided the draft decision to Ryanair to allow it to make submissions. Ryanair subsequently provided a number of submissions, which (along with the DPC's analysis thereof) were taken into account in the draft decision.

(ii) Provision of Draft Decision to Concerned Supervisory Authorities

In accordance with the Article 60 process, the DPC proceeded to submit its draft decision to the IMI to be circulated amongst the Concerned Supervisory Authorities (CSAs), pursuant to Article 60(3) of the GDPR. The DPC's draft decision was uploaded to the IMI on 25 May 2020 and, pursuant to Article 60(4) of the GDPR, the CSAs were thereafter entitled to four weeks in which to submit any relevant and reasoned objections to the decision.

The DPC subsequently received a number of relevant and reasoned objections and comments in relation to its draft decision from the CSAs. In particular, certain CSAs argued that additional infringements of the GDPR ought to have been found, and in addition that a reprimand ought to have been imposed.

(iii) Revised Draft Decision

In accordance with Article 60(3) of the GDPR, the DPC is obliged to take due account of the views of the CSAs. In light of the objections and comments received from the CSAs, the DPC carefully considered each relevant and reasoned objection and comment received in respect of its draft decision. The DPC revised its draft decision to include a summary and analysis of the objections and comments expressed by the CSAs. In revising its initial draft, the DPC followed certain relevant and reasoned objections received, and declined to follow others. In the its revised draft decision, the DPC proposed to issue a reprimand to Ryanair, pursuant to Article 58(2) (b) of the GDPR. The DPC provided its revised draft decision to Ryanair to allow it to make final

submissions. Ryanair noted that the DPC had found that it had infringed the GDPR, and that the DPC had exercised its powers in this case in line with Recital 129 and the due process requirements in Article 58 of the GDPR. Ryanair advised the DPC that it accepted the findings and the associated reprimand and did not wish to make any further submissions.

(iv) Provision of Revised Draft Decision to Concerned Supervisory Authorities

In accordance with Article 60(5) of the GDPR, once the DPC submitted its revised draft decision to the CSAs for their views, the CSAs were entitled to two further weeks in which to submit any further objections to the decision.

Pursuant to Article 60(5) of the GDPR, the DPC submitted its revised draft decision to the CSAs for their opinion on 20 October 2020. As the DPC received no further objections or comments in relation to the revised draft decision from the CSAs within the statutory period, the CSAs were deemed to be in agreement with the revised draft decision of the DPC and bound by it in accordance with Article 60(6) of the GDPR.

(v) Adoption of Final Decision

Upon the passing of the deadline for receipt of any further objections, the DPC proceeded to adopt the final decision, in accordance with Article 60(7) of the GDPR. The DPC then uploaded its final decision to the IMI and communicated it to Ryanair. The final decision was uploaded on 11 November 2020. Pursuant to Article 60(7), the ICO, with whom the complaint was initially lodged, was responsible for informing the complainant of the decision.

In summary, the DPC found infringements of Articles 12(3) and Article 15 of the GDPR in respect of this complaint.

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.

This case study also demonstrates — once again — the intensity of DPA resources consumed in delivering outcomes on issues that could have been resolved by the controller without recourse to the DPC, raising again the question of unwarranted DPA resource-drainage away from resolving wider systemic issues which would achieve improved outcomes for the maximum number of individuals.

Case Study 11:

Purpose Limitation — Law Enforcement Directive

The DPC examined a complaint where an individual alleged that data gathered in one particular law enforcement context was being used by the same data controller for another law enforcement purpose. The complaint concerned the prosecution of an individual for offences in the equine and animal remedies area by the Department of Agriculture, Food & the Marine (DAFM) and the separate referral by DAFM of allegations of professional misconduct to the Veterinary Council of Ireland (VCI) in relation to the same person.

Having examined the matters raised, the DPC referred the complainant to Section 71(5) of the Data Protection Act 2018:

Where a controller collects personal data for a purpose specified in section 70 (1)(a), the controller or another controller may process the data for a purpose so

specified other than the purpose for which the data were collected, in so far as—

(a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and

(b) the processing is necessary and proportionate to the purpose for which the data are being processed.

With regard to section 70(1)(a) and “the law of the State”, the DPC noted the provisions set out in the Veterinary Practice Act 2005 regarding the conduct of inquiries by the VCI into allegations of professional misconduct. In particular, section 76 of the Veterinary Practice Act 2005 outlines that the VCI or any person may apply for an inquiry with regards to the fitness to practice veterinary medicine of a registered person. On this basis, the DPC did not consider data protection legislation to disallow the separate referral by DAFM of allegations of professional misconduct to the VCI 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.

Case Study 12:

Alleged disclosure of the complainant's personal data by a local authority (Data Breach Complaint)

The DPC received a complaint from an individual concerning an alleged disclosure of the complainant's personal data by a local authority. The complainant alleged that the local authority had disclosed the complainant's name, postal address and information relating to the housing assistance payment in error to a third-party. The individual had been informed by the local authority that this disclosure had occurred. However, the individual was dissatisfied with the actions taken by the local authority in response to the disclosure and did not wish to engage further with the local authority with a view to seeking an amicable resolution of the complaint.

The DPC examined the complaint and contacted the local authority in order to seek further information regarding the individual's allegations. The local authority confirmed to the DPC that a personal data breach had occurred when the complainant's personal data was included, in error, in a Freedom of Information request response to a third-party.

In addition to the information provided by the local authority to the DPC in the context of its examination of the complaint, the incident in question was notified to the DPC by the local authority as a personal data breach, as required by Article 33 of the GDPR. In that context, the DPC engaged extensively with the local authority regarding the circumstances of the personal data breach, the data security measures in place at the time the personal data breach occurred and the mitigating measures taken by the local authority, including the local authority's ongoing efforts to retrieve the data from the recipient.

On the basis of this information, the DPC concluded its examination of the complaint by advising the individual that the DPC was satisfied that the complainant's 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. On the basis of the actions that had been taken by the local authority in response to the personal data breach and, in particular, the fact that the recipient of the complainant's personal data had returned the data to the local authority, the DPC did not consider that any further action against the local authority was warranted in relation to the subject matter of the complaint.



3

Breaches

Breaches under the GDPR

In 2020, the DPC received, 6,783 data-breach notifications under Article 33 of the GDPR, of which, 110 cases (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) of the GDPR. A total of 6,673 valid data protection breaches were recorded by the DPC in 2020, representing an increase of 10% (604) on the numbers reported in 2019.

As in other years, the highest category of data breaches notified under the GDPR were classified as Unauthorised Disclosures and accounted for 86% of the total data-breach notifications received in 2020. The majority occurred in the:

Private Sector	4097
Public Sector	2559
Voluntary	16
Charity	1
Total	6673

The DPC also saw an increase in the use of social engineering and phishing attacks to gain access to the ICT systems of controllers and processors. While many organisations initially put in place effective ICT security measures, it is evident that organisations are not taking proactive steps to monitor and review these measures, or to train staff to ensure that they are aware of evolving threats. In these instances, we continue to recommend that organisations undertake periodic reviews of their ICT security measures and implement a comprehensive training plan for employees supported by refresher training and awareness programmes to mitigate the risks posed by an evolving threat landscape.

Data breach notifications by category	Private	Public	Total
Disclosure (unauthorised)			5,837
Hacking			146
Malware			19
Phishing -incl. social engineering			74
Ransomware/denial of service			32
Software Development Vulnerability			5
Device lost or stolen (encrypted)			19
Device lost or stolen (unencrypted)			29
Paper lost or stolen			275
E-waste (personal data present on an obsolete device)			1
Inappropriate disposal of paper			21
System Misconfiguration			40
Unauthorised Access			146
Unintended online publication			61
Other			78
Total			6,783

E-Privacy Breaches

The DPC received a total of **70 valid data-breach notifications under the e-Privacy Regulations** (S.I. No. 336 of 2011), which accounted for just over 1% of total valid cases notified for the year.

Led Breaches

The DPC also received **25 breach notifications in relation to the LED**, (Directive (EU) 2016/680), which has been transposed into Irish law by certain parts of the Data Protection Act 2018.

DPC Assessment of a breach

Once a breach notification is lodged with the DPC, the DPC assesses it taking account of multiple aspects of the breach and the risks it poses. The first of these is the nature of the breach, including whether it was intentionally or accidentally caused, whether data was exfiltrated or made inaccessible, and the modes of technology and organisation involved. A history of breaches of a particular type may indicate a systemic issue affecting an individual data controller, a particular location or an entire economic sector.

Characteristics of the personal data involved are central to the DPC's assessment. These include the types, format and sensitivity of the personal data, the number of persons and records affected, and the potential for the data to be read or disseminated. The DPC will look at whether aspects such as profiling, automated decision making, monitoring or tracking has been taking place.

Similarly, categorisation of the data subjects — such as whether they are children or vulnerable persons — and characteristics of the data controller and/or processor, such as statutory responsibilities or processing of other types of personal data, can be highly significant. The volume of data subjects and the location of these data subjects is taken into account.

Other factors to be considered are the potential harms to data subjects resulting from disclosure, misuse or loss of personal data affected by the breach. This aspect of risk assessment is often overlooked by data controllers. Harms can range from temporary inconvenience to very serious risks, such as identity theft, financial loss, and misdiagnosis of medical conditions or reputational damage. The DPC will consider what the impact to the affected individuals is, including the severity, scope and context of the persons.

Finally, the DPC assesses mitigating factors, such as whether backups are available, vulnerabilities are addressed, and whether the data is retrieved or further disclosure prevented. Often data controllers do not implement simple measures such as encryption of information shared via email, ensuring that all IT security measures are in place but also kept regularly updated. These factors are taken into consideration in the assessment.

If the facts are not fully known or remain unclear after the DPC's initial assessment of a breach, they will continue to engage with the controller until such time as all matters have been responded to, to the satisfaction of the DPC. In some cases, the controller or processor may be asked to reassess the causes and consequences of the breach and report on its findings. Breaches involving complex IT issues may require assessment and analysis by the DPC's technical specialists. In cases where the controller has either produced or commissioned a technical report or investigation report on the breach, a copy of this will be requested.

Pending completion of its investigation, the DPC may direct and monitor progress — on a rolling basis — of measures implemented to remedy or mitigate the effects of the breach. These could include informing data subjects of the breach under Article 34 of the GDPR, or the implementation of technical or organisational measures to address vulnerabilities.

Based on its assessment and on the controller's actions to prevent or mitigate against further similar incidents, the DPC may conclude its investigation at this point. If the DPC is not satisfied with the mitigations or responses from the controller, it can escalate the matter for further investigative/enforcement action.

Case Studies

Case Study 13:

Breach Notification (Voluntary Sector) — Ransomware Attack

In May 2020, the DPC received a breach notification from an Irish data processor and subsequently a notification from an Irish data controller operating in the voluntary sector 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, and which was the result of malware gaining access via an RDP⁴ port to the server.

⁴ RDP — Remote desktop protocol

The DPC engaged with both the controller and processor and through a number of communications — including the issuing of technical and organisational questionnaires focusing on areas of potential non-compliance with data protection regulation. These areas included the processor's use of a data centre within the US to store back-up data without adequate agreements — and sufficient oversight by the controller over its processor — as required under Article 28 of the GDPR.

The DPC engaged intensively with both parties and the DPC concluded this case by issuing recommendations to both controller and processor. Thereafter the DPC continued to engage with both parties to ensure that implementation of the DPC recommendations had occurred.

Case Study 14:

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 (Twitter).

The personal data was posted in violation of its policy to anonymise all content, which could potentially identify an individual data subject. The organisation in question informed the DPC that the root cause of this incident was human error and the offending tweet was removed without undue delay.

Based on the action the data controller had taken to mitigate against the risk of this type of incident reoccurring the DPC concluded its examination of this matter and issued a number of further recommendations to the organisation centring on the appropriate use of its social media platforms and how its social media accounts should be secured and limited to a specified number of authorised personnel.

Case Study 15:

Breach Notification (Financial Sector) Bank Details sent by WhatsApp

A private financial sector organisation notified the DPC that a customer had made a request to obtain their IBAN and BIC numbers which were held on file. The customer making the request was personally known to the member of staff dealing with the request. The member of staff, deviating from approved practices, used their personal mobile phone to send a picture of what they believed to be the requested information over a messaging platform (WhatsApp). However the staff member erroneously sent details pertaining to another customer to the requesting customer.

The customer who received this information contacted the organisation to advise that the information received did not relate to their account and that they had undertaken to delete all offending material from their device. The organisation communicated with staff to remind them that only authorised methods of communication should be utilised when handling future requests of this nature. The organisation has also issued an apology to all affected data subjects.

The DPC issued a number of recommendations encompassing the use of only approved organisational communication tools, making staff fully aware of acceptable and non-acceptable behaviour when using organisational communications tools, and to ensure staff have undergone appropriate training in terms of their obligations/responsibilities under the provisions of the GDPR and the Data Protection Act 2018.

Case Study 16:

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 when implementing measures introduced in response to the Covid-19 pandemic.

Credit unions are required to report information to the Central Bank of Ireland concerning their borrowers and the performance of their loans. The Central Bank utilises this information to maintain the Central Credit Register (or CCR). Lenders and credit rating agencies in turn use this information to verify borrowers' debts and credit histories. A large number of lenders, particularly credit unions, use the services of data processing companies to prepare such CCR returns and forward them to the Central Bank.

During 2020, the Irish Government introduced a series of measures to mitigate financial distress caused by the pandemic and resulting lock-downs. These included measures allowing financial institutions to pause loan repayments without adversely affecting borrowers' credit ratings. Lenders were instructed to use particular codes in the CCR returns to flag paused loans. This was intended to prevent those loans being interpreted as delinquent or otherwise suggesting that the relevant borrowers' credit-worthiness had deteriorated.

In this incident the processor employed by the 12 credit unions used incorrect codes on CCR returns dealing with paused loans. The incorrect codes indicated that the borrowers affected had undergone a 'restructuring event' — a restructuring event typically occurs when a borrower is unable to repay a loan over the agreed period, and the lender agrees to change the loan's terms to improve the borrower's ability to repay. This can greatly reduce a borrower's credit rating, so an inaccurate CCR record of a restructuring event could have serious consequences for the persons affected.

The credit unions in question became aware of the processor's coding error in relation to their CCR returns several weeks after the processor first sent CCR returns for them using the incorrect codes to the Central Bank. The issue was reported to the DPC as a breach and credit unions took the matter up with the processor directly and through a user group. This allowed affected records to be identified, the appropriate coding procedures to be worked out, and corrected CCR returns to be sent to the Central Bank.

These cases illustrate the importance of processing contracts that properly implement the requirements of Article 28 of the GDPR. Most relevantly to these cases, 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.



4

Inquiries

On 31 December 2020, the DPC had **83 statutory inquiries on hand, including 27 cross-border inquiries.**

Cross-Border Statutory Inquiries commenced since 25 May 2018

Company	Inquiry type	Issue being examined
Apple Distribution International	Complaint-based	<i>Lawful basis for processing.</i> Examining whether Apple has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of behavioural analysis and targeted advertising on its platform.
Apple Distribution International	Complaint-based	<i>Transparency.</i> Examining whether Apple has discharged its GDPR transparency obligations in respect of the information contained in its privacy policy and online documents regarding the processing of personal data of users of its services.
Apple Distribution International	Complaint-based	<i>Right of Access.</i> Examining whether Apple has complied with the relevant provisions of the GDPR in relation to an access request for customer service related personal data.
Facebook Inc.	Own-volition	<i>Facebook September 2018 token breach.</i> Examining whether Facebook Inc. has discharged its GDPR obligations to implement organizational and technical measures to secure and safeguard the personal data of its users.
Facebook Ireland Limited	Complaint-based	<i>Right of Access and Data Portability.</i> Examining whether Facebook has discharged its GDPR obligations in respect of the right of access to personal data in the Facebook 'Hive' database and portability of "observed" personal data.
Facebook Ireland Limited	Complaint-based	<i>Lawful basis for processing in relation to Facebook's Terms of Service and Data Policy.</i> Examining whether Facebook has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data of individuals using the Facebook platform.
Facebook Ireland Limited	Complaint-based	<i>Lawful basis for processing.</i> Examining whether Facebook has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of behavioural analysis and targeted advertising on its platform.
Facebook Ireland Limited	Own-volition	<i>Facebook September 2018 token breach.</i> Examining whether Facebook Ireland has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.
Facebook Ireland Limited	Own-volition	<i>Facebook September 2018 token breach.</i> Examining Facebook's compliance with the GDPR's breach notification obligations

Company	Inquiry type	Issue being examined
Facebook Ireland Limited	Own-volition	<i>Commenced in response to large number of breaches notified to the DPC during the period since 25 May 2018 (separate to the token breach).</i> Examining whether Facebook has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.
Facebook Ireland Limited	Own-volition	Facebook passwords stored in plain text format in its internal servers. Examining Facebook's compliance with its obligations under the relevant provisions of the GDPR
Facebook Ireland Limited	Own-volition	Inquiry examining Facebook Ireland Limited's compliance with Chapter V GDPR (in particular Article 46) in light of the judgment of the CJEU on 16.07.20
Google Ireland Limited	Own-volition	Commenced in response to submissions received. Examining Google's compliance with the relevant provisions of the GDPR. The GDPR principles of transparency and data minimisation, as well as Google's retention practices, will also be examined.
Google Ireland Limited	Own-volition	Examining whether Google has a valid legal basis for processing the location data of its users and whether it meets its obligations as a data controller with regard to transparency.
Instagram (Facebook Ireland Limited)	Complaint-based	<i>Lawful basis for processing in relation to Instagram's Terms of Use and Data Policy.</i> Examining whether Instagram has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data of individuals using the Instagram platform
Instagram (Facebook Ireland Limited)	Own-volition	Inquiry in respect of Facebook's compliance with its GDPR obligations regarding its processing of personal data of Instagram users under the age of 18 ("Child Users") in connection with account settings
Instagram (Facebook Ireland Limited)	Own-volition	Inquiry in respect of Facebook's compliance with its GDPR obligations regarding its reliance on legal bases pursuant to Article 6 of the GDPR for the processing of personal data of Instagram users under the age of 18 ("Child Users").
LinkedIn Ireland Unlimited Company	Complaint-based	<i>Lawful basis for processing.</i> Examining whether LinkedIn has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data in the context of behavioural analysis and targeted advertising on its platform.

Company	Inquiry type	Issue being examined
MTCH Technology Services Limited (Tinder)	Own-volition	Examining whether the company has a legal basis for the ongoing processing of its users' personal data and whether it meets its obligations as a data controller with regard to transparency and its compliance with data subject rights requests.
Quantcast International Limited	Own-volition	Commenced in response to a submission received. Examining Quantcast's compliance with the relevant provisions of the GDPR. The GDPR principle of transparency and retention practices will also be examined.
Twitter International Company	Complaint-based	<i>Right of Access.</i> Examining whether Twitter has discharged its obligations in respect of the right of access to links accessed on Twitter.
Twitter International Company	Own-volition	Commenced in response to the large number of breaches notified to the DPC during the period since 25 May 2018. Examining whether Twitter has discharged its GDPR obligations to implement organisational and technical measures to secure and safeguard the personal data of its users.
Twitter International Company	Own-volition	Commenced in response to a breach notification. Examining an issue relating to Twitter's compliance with Article 33 of the GDPR.
Verizon Media/Oath	Own-volition	<i>Transparency.</i> Examining the company's compliance with the requirements to provide transparent information to data subjects under the provisions of Articles 12-14 GDPR.
WhatsApp Ireland Limited	Complaint-based	<i>Lawful basis for processing in relation to WhatsApp's Terms of Service and Privacy Policy.</i> Examining whether WhatsApp has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data of individuals using the WhatsApp platform.
WhatsApp Ireland Limited	Own-volition	<i>Transparency.</i> Examining whether WhatsApp has discharged its GDPR transparency obligations with regard to the provision of information and the transparency of that information to both users and non-users of WhatsApp's services, including information provided to data subjects about the processing of information between WhatsApp and other Facebook companies.
Yelp	Own-volition	Inquiry into Yelp's compliance with Articles 5, 6, 7 and 17 of GDPR following a number of complaints received by the DPC in relation to the processing of personal data by Yelp on its website.

Domestic Statutory Inquiries commenced since 25 May 2018

Company	Inquiry type	Issue being examined
31 local authorities and An Garda Síochána	Own Volition	Examining surveillance of citizens by the state sector for law enforcement purposes through the use of technologies such as CCTV, body-worn cameras, automatic number plate recognition (ANPR) enabled systems, drones and other technologies. The purpose of these inquiries is to probe whether the processing of personal data that occurs in those circumstances is compliant with data protection law.
An Garda Síochána	Own Volition	Examining governance and oversight with regard to disclosure requests within AGS and within organisations processing such requests, as well as examining the actual requests made by AGS to third parties.
An Garda Síochána	Own Volition	Examining a breach of security resulting in a potential unauthorised disclosure of personal data held for LED processing.
Bank of Ireland	Own Volition	Commenced in response to the large number of data breaches notified to the DPC during the period since 25 May 2018.
Bank of Ireland	Own Volition	Examining a potential unauthorised disclosure of personal data in how BOI provisioned certain Banking 365 customers. There were multiple incidents involving the bank misconfiguring a new customer's 365 profile such that a customer could inadvertently access the personal data and current account of a different customer.
BEO Solutions	Own Volition	Examining a personal data breach notified in connection with the loss of a USB storage device. Related to inquiry into PIAB.
Catholic Church	Own Volition	Examining multiple complaints regarding compliance with requests for the right to rectification & right to be forgotten
Department of Social Protection (Formerly DEASP)	Own Volition	Examining the position of the Data Protection Officer under Article 38 of the GDPR.
Department of Social Protection Formerly (DEASP)	Own Volition	Examining whether certain processing and/or proposed processing of personal data by the Department in the context of ongoing eligibility assessments/checks for child benefit is compliant with the GDPR and with the Data Protection Act 2018.
HSE Mid Leinster (Tullamore Labs)	Own Volition	Commenced in response to a breach notified to the DPC.

Company	Inquiry type	Issue being examined
HSE Our Lady of Lourdes	Own Volition	Examining the security of processing data, appropriate organisational and technical measures following the loss of sensitive personal data.
HSE South	Own Volition	Commenced in response to a breach notified to the DPC.
Irish Credit Bureau	Own Volition	Commenced in response to a breach notified to the DPC.
Irish Prison Service	Own Volition	Examining whether the IPS has discharged its GDPR obligations in respect of the lawful basis on which it relies to process personal data
Maynooth University	Own Volition	Commenced in response to a breach notified to the DPC in relation to a phishing incident.
Move Ireland Limited	Own Volition	Examining compliance with GDPR obligations in relation to the loss of recorded counselling sessions involving sensitive personal data.
Personal Injuries Assessment Board	Own Volition	Examining compliance with GDPR obligations in relation to a personal data breach notified which occurred through the loss of a USB storage device. Related to inquiry into BEO Solutions.
Slane Credit Union	Own Volition	Commenced in response to a breach notified to the DPC in relation to an unauthorised disclosure.
SUSI	Own Volition	Commenced in response to a breach notified to the DPC.
Teaching Council	Own Volition	Examining compliance with GDPR obligations in connection with the phishing of two email accounts held by staff of the Council, email redirection rules were set which caused the unauthorized processing of 332 emails containing personal data of a large number of data subjects.
TUSLA	Own Volition	Commenced in response to a number of breaches notified to the DPC.
TUSLA	Own Volition	Commenced in response to a number of breaches notified to the DPC during the period since 25 May 2018.
TUSLA	Own Volition	Commenced in response to a breach notified to the DPC.
UCD	Own Volition	Commenced in response to a number of breaches notified to the DPC during the period since 25 May 2018.
University of Limerick	Own Volition	Commenced in response to a breach notified to the DPC in relation to a phishing incident.



5

Decisions

Decisions under the Data Protection Act 2018

The DPC decides, on foot of statutory inquiries, whether infringements of data protection legislation have occurred. These statutory inquiries include own volition inquiries and inquiries on foot of complaints. Where infringements are found, the decision-maker also makes a decision as to whether a corrective power should be exercised, and, if so, the corrective power(s) that are to be exercised.

Where the DPC decides to impose an administrative fine, and if there is no appeal against that decision, the DPC must make an application in a summary manner to the Circuit Court for confirmation of the decision to impose an administrative fine pursuant to Section 143(1) of the Data Protection Act 2018. Section 143(2) provides that the Circuit Court shall confirm the decision unless it sees good reason not to. All DPC fines are remitted to the Exchequer on receipt in accordance with Section 141(7) of the Data Protection Act 2018.

Organisations	Decision Issued
Kerry County Council	25-Mar-20
Waterford City and County Council	21-Oct-20
Tusla Child and Family Agency (3 breaches)	07-Apr-20
Tusla Child and Family Agency (1 breach)	21-May-20
Tusla Child and Family Agency (71 breaches)	12-Aug-20
Health Service Executive (HSE South)	18-Aug-20
Health Service Executive (Our Lady of Lourdes Hospital)	29-Sep-20
Ryanair	11-Nov-20
Twitter International Company	9-Dec-20
Groupon	16-Dec-20
University College Dublin	17-Dec-20

Kerry County Council

In March 2020, the DPC issued a decision to Kerry County Council in respect of one of a number of own-volition inquiries it has undertaken concerning Local Authorities. These inquiries consider a broad range of issues pertaining to surveillance technologies deployed by State authorities. The inquiry was conducted initially by means of an audit under Section 136 of the Data Protection Act 2018. This facilitated the DPC in compiling facts in relation to the deployment of surveillance technologies by the Council. The DPC final inquiry report was completed on 4 October 2019 and submitted to the decision-maker (the Commissioner).

This decision found that certain CCTV systems operated by Kerry County Council were unlawful in the absence of authorisation from the Garda Commissioner under Section 38 of An Garda Síochána Act 2005. Significantly, the Litter Pollution Act 1997, the Waste Management Act 1996, and the Local Government Act 2001 were comprehensively considered and the decision found that those Acts do not provide a lawful basis for the use of CCTV for law enforcement purposes.

The decision also considered signage used by the Council to notify the public of its use of CCTV, finding that some of the signage was inadequate in light of the requirements of the Data Protection Act 2018. The decision considered the field of vision of CCTV operated by the Council and found that, in the absence of privacy masking, the data collection was excessive in some locations where the CCTV also captured private residences. The decision also made findings in relation to the 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; the practice of sharing login details for accessing CCTV footage; security measures for trans-

ferring CCTV footage to An Garda Síochána; and the requirement for Data Protection Impact Assessments.

The decision imposed a temporary ban on Kerry County Council's processing of personal data in respect of certain CCTV cameras. The decision also ordered the Council to bring its processing into compliance by taking specified action and reprimanded the Council in respect of the infringements. On 27 April 2020, the Kerry County Council lodged an appeal against the decision to the Circuit Court. On 8 September 2020, Kerry County Council withdrew the appeal, accepting the findings in the decision.

Waterford City and County Council

In October 2020, the DPC issued a decision to Waterford City and County Council in respect of another inquiry concerning surveillance technologies deployed by State authorities. The inquiry was conducted initially by means of an audit under Section 136 of the Data Protection Act 2018. This facilitated the DPC in compiling facts in relation to the deployment of surveillance technologies by the Council. The final inquiry report was completed on 24 October 2019 and submitted to the decision-maker (the Commissioner).

The decision found that Waterford City and County Council's use of dash cams and covert cameras to detect littering and dumping for law enforcement purposes do not have a lawful basis in the Litter Pollution Act 1997 and the Waste Management Act 1996. The decision also found that certain CCTV cameras operated by the Council for crime prevention were unlawful in the absence of authorisation from the Garda Commissioner under Section 38 of An Garda Síochána Act 2005.

The decision found that An Garda Síochána and Waterford City and County Council are joint controllers in respect of certain CCTV cameras authorised under Section 38(3)(c) of An Garda Síochána Act 2005. In this regard, the decision found that Waterford City and County Council infringed Section 79 of the Data Protection Act 2018 by failing to implement an agreement in writing with An Garda Síochána. The decision also made findings on the adequacy of Waterford City and County Council's policy in respect of its use of drones for monitoring compliance on permitted waste sites and preventing dumping on illegal waste sites, and its obligation to maintain a data log for specific accesses to CCTV recordings.

The decision imposed a temporary ban on Waterford City and County Council's processing of personal data by means of certain overt CCTV cameras, dash cams for law enforcement purposes, and covert cameras. The decision also ordered the Council to bring its processing into compliance by taking specified action and reprimanded the Council in respect of the infringements. Waterford City and County Council did not appeal against this decision.

Tusla — April 2020

In April 2020, the DPC issued a decision in respect of an own-volition inquiry regarding three personal data breaches notified to the DPC by Tusla. These breaches occurred when Tusla failed to redact documents when sharing them with third parties. The first personal data breach occurred when Tusla unintentionally provided the father of two children in care with their foster carer's address. The second breach occurred when Tusla unintentionally provided an individual who was accused of child sexual abuse with the address of the child who made the complaint and with her mother's telephone number. The third breach occurred when Tusla unintentionally provided the grandmother of a child in care with the address and contact details of the child's foster parents and the location of the child's school.

The inquiry commenced on 24 October 2019 and examined whether Tusla had discharged its obligations in connection with the breaches, in order to determine whether any provision(s) of the GDPR and/or the Data Protection Act 2018 had been contravened by Tusla. The final inquiry report was completed on 24 February 2020 and submitted to the decision-maker (the Commissioner).

The decision considered the appropriateness of the technical and organisational measures implemented by Tusla at the time of the breaches. The decision found that Tusla infringed Article 32(1) of the GDPR by failing to implement appropriate measures with regard to the redaction of documents. The decision also considered one of the notified personal data breaches with regard to the duty to notify the DPC without undue delay pursuant to Article 33(1) of the GDPR. Tusla notified the DPC of this breach 5 days after becoming aware of it. The decision found that this constituted an undue delay in the circumstances and found that Tusla had infringed Article 33(1).

The decision reprimanded Tusla, ordered it to bring its processing into compliance with Article 32(1) of the GDPR, and imposed an administrative fine of €75,000. No appeal was taken by Tusla against the DPC's decision. On 4 November 2020, the DPC made an application to the Circuit Court to confirm its decision in this inquiry to impose the administrative fine. The Circuit Court confirmed the decision pursuant to Section 143 of the Data Protection Act 2018.

Tusla — May 2020

In May 2020, the DPC issued a decision regarding another own-volition inquiry concerning Tusla. This inquiry concerned one personal data breach that Tusla notified to the DPC on 4 November 2019. The inquiry commenced on 11 December 2019 and examined whether Tusla had discharged its obligations in connection with the subject matter of the breach to determine whether any provision(s) of the GDPR and/or the Data Protection Act 2018 had been contravened by Tusla.

The breach occurred when Tusla wrote a safeguarding letter to a third party that included the identity of individuals who had made allegations of abuse and the details of the allegations made. The letter disclosing the details was later shared on social media by the recipient of the letter. On 19 March 2020, the final inquiry report was completed and submitted to the decision-maker (the Commissioner).

The decision considered the appropriateness of the technical and organisational measures implemented by Tusla at the time of the breach in respect of its safeguarding letter process. It found that Tusla infringed Article 32(1) of the GDPR by failing to implement organisational measures appropriate to the risk. The decision also considered the breach with regard to the duty to notify the DPC without undue delay pursuant to Article 33(1) of the GDPR. This breach was notified to the DPC over 29 weeks after Tusla became aware of it. The decision found that Tusla infringed Article 33(1) by failing to notify the DPC of the breach without undue delay. The decision reprimanded Tusla, ordered it to bring its processing into compliance, and imposed an administrative fine of €40,000. Tusla did not appeal against this decision. At the time of writing, the DPC's application before the Circuit Court to confirm the administrative fine is pending.

Tusla — August 2020

In August 2020, the DPC issued a decision in respect of an own-volition inquiry regarding 71 personal data breaches notified to the DPC by Tusla. The relevant breaches occurred between 25 May 2018 to 16 November 2018 and they all concerned the unauthorised disclosure of, or access to, personal data processed by Tusla. The inquiry commenced on 6 December 2018 and examined whether Tusla discharged its obligations in connection with the subject matter of the breaches to determine whether any provision(s) of the GDPR and/or the Data Protection Act 2018 had been contravened by Tusla. The final inquiry

report was completed on 3 April 2020 and submitted to the decision-maker (the Commissioner).

The decision made findings in relation to security of processing, personal data accuracy, and Tusla's obligation to notify personal data breaches without undue delay. Regarding security of processing, the decision found five distinct infringements of Article 32(1) of the GDPR in respect of Tusla's obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its various processing operations. The processing operations under consideration concerned Tusla's transmission of personal data on its internal information system; Tusla's transmission of personal data internally by email; Tusla's transmission of personal data externally using post and email; Tusla's printing and scanning; and Tusla's record management and information handling. The decision found that Tusla infringed Article 32(4) of the GDPR by failing to take steps to ensure that persons acting under its authority do not process certain personal data except on instructions from Tusla. The decision also found that Tusla infringed Article 5(1)(d) of the GDPR on four occasions by failing to ensure that the personal data that it processed was accurate and, where necessary, kept up to date. Finally, the decision found that Tusla infringed Article 33(1) by failing to notify the DPC of personal data breaches without undue delay on 8 occasions.

The decision reprimanded Tusla in respect of its infringements of Articles 5(1)(d), 32(1), 32(4), and 33(1) of the GDPR. The decision also ordered Tusla to bring its processing into compliance with Article 32(1) of the GDPR by implementing specified appropriate technical and organisational measures to ensure a level of security appropriate to the risks identified.

In circumstances where some of the infringements concerned the same or linked processing operations, and where one of the infringements of Article 32(1) was not linked to the other processing operations under consideration in the decision, the decision found that it was appropriate to impose two separate administrative fines on Tusla. The decision imposed one administrative fine in the amount of €50,000, and one administrative fine in the amount of €35,000. Tusla did not appeal against this decision. At the time of writing, the DPC's applications before the Circuit Court to confirm the administrative fines are pending.

HSE — August 2020 & September 2020

In August 2020, the DPC issued a decision in respect of an own volition inquiry regarding a personal data breach notified by the Health Service Executive (HSE) to the DPC on 14 June 2019. The personal data breach occurred when documentation containing the personal data of 78 data subjects, including special category personal data in respect of six of those data subjects, was disposed of in a public recycling centre. The documentation was created in Cork University Maternity Hospital, but was discovered by a member of the public in the public recycling area. The inquiry commenced on 17 October 2019 and examined whether the HSE discharged its obligations in connection

with the subject matter of that personal data breach and to determine whether any provision(s) of the Data Protection Act 2018 and/or the GDPR were contravened by the HSE in that context. The final inquiry report was completed on 27 April 2020 and submitted to the decision-maker (the Commissioner).

In September 2020, the DPC issued a decision regarding another own-volition inquiry concerning the HSE. The inquiry concerned a personal data breach that the HSE notified to the DPC on 1 May 2019. That personal data breach occurred in circumstances where a member of the public informed the HSE that they had found documents in their front garden, which is near Our Lady of Lourdes Hospital. The documents in question were handover notes, generated by the HSE to identify patients who come under staff care at each shift change. The notes are necessary for continuing patient care and treatment. The notes contained the personal data of 15 data subjects and included data relating to clinical information and treatments received. The notes were printed on 11 April 2019, but the HSE was unable to specify the date on which the breach initially occurred. The notes had not been accounted for between the date they were printed and when they were found. The inquiry commenced on 26 November 2019 and examined whether the HSE discharged its obligations in connection with the subject matter of that personal data breach to determine whether any provision(s) of the Data Protection Act 2018 and/or the GDPR had been contravened by the HSE in that context.

The August 2020 decision found that the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its use and disposal of hardcopy documents containing patients' personal data. The decision imposed an administrative fine of €65,000 on the HSE for its infringements of Articles 5(1)(f) and 32(1) of the GDPR. 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 Articles 5(1)(f) and 32(1) of the GDPR by implementing certain specified measures. The HSE did not appeal against this decision. At the time of writing, the DPC's application before the Circuit Court to confirm the administrative fine is pending.

Similarly, the September 2020 decision found that the HSE infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by its use and disposal of hardcopy documents containing patients' personal data. Having regard to the order, the reprimand, and the fine imposed in respect of the HSE decision in August 2020, the DPC found that it was not appropriate to exercise further corrective powers in this Decision. The finding of infringements in both decisions concerned the same processing operations, undertaken by the same controller, during the same time-period.

Twitter International Company — December 2020

In December 2020, the DPC issued a decision regarding an own-volition inquiry concerning Twitter International Company ('TIC'). The inquiry commenced on 22 January 2019 and concerned the question of TIC's compliance with its obligations under Articles 33(1) and 33(5) GDPR in respect of the notification and documentation of a personal data breach. The personal data breach arose from a bug in the Twitter mobile app for Android which meant that any user that changed the email address associated with their account automatically had all of their "protected" (only visible to their "followers") tweets made publicly accessible.

The decision found that TIC infringed Article 33(1) of the GDPR by failing to notify the DPC of the personal data breach without undue delay. In terms of the timeline of the notification, the personal data breach was discovered by a data sub-processor on 26 December 2018, and was deemed to be a potential data breach under the GDPR by the wider Twitter organisation on 3 January 2019. There was, however, a delay (until 7 January 2019) in notifying TIC (as controller) and the Global DPO of the breach, which arose out of a failure by employees of Twitter Inc. to follow internal guidance. During the inquiry, TIC submitted that, in circumstances where it had notified the breach to the DPC on 8 January 2019, it had complied with its obligations under Article 33(1).

The decision, in finding an infringement of Article 33(1), outlined that TIC (as controller) could not seek to rely on a failure by its processor to follow an internal process and / or an ineffectiveness in that process in order to avoid responsibility under Article 33(1) of the GDPR for delayed notification of the breach to the DPC. The decision also found that TIC infringed Article 33(5) of the GDPR by failing to adequately document the personal data breach.

The DPC submitted its draft decision in this inquiry to other Concerned Supervisory Authorities (CSAs) under Article 60 GDPR on 22 May 2020. This was the first draft decision to go through the Article 65 dispute resolution process and was the first draft decision in a "big tech" case on which all EU supervisory authorities were consulted as CSAs. The European Data Protection Board adopted its decision under Article 65(1)(a) on 9 November 2020. The DPC issued its final decision to TIC on 9 December 2020. That decision imposed an administrative fine of \$500,000 (estimated for this purpose at €450,000) on Twitter as an effective, proportionate and dissuasive measure.

UCD — December 2020

In December 2020, the DPC issued a decision regarding an own-volition inquiry concerning University College Dublin ('UCD'). This inquiry concerned seven personal data breaches that UCD notified to the DPC between 8 August 2018 and 21 January 2019. The inquiry commenced on 19 July 2019 and examined whether UCD had discharged its obligations in connection with the subject matter of the breaches and determine whether or

not any provision(s) of the 2018 Act and/or the GDPR had been contravened by UCD in that context.

The personal data breaches concerned instances where unauthorised third parties accessed UCD email accounts, or where the login credentials for UCD email accounts were posted online. On 8 July 2020, the DPC completed the final inquiry report and submitted it to the decision-maker (the Commissioner).

The decision considered the appropriateness of the technical and organisational measures implemented by UCD at the time of the breaches in respect of its email service. It found that UCD infringed Articles 5(1)(f) and 32(1) of the GDPR by failing to process personal data on its email service in a manner that ensured appropriate security of the personal data using appropriate technical and organisational measures. The decision also found that UCD infringed Article 5(1)(e) of the GDPR by storing certain personal data in an email account in a form which permitted the identification of data subjects for longer than necessary for the purpose for which the personal data were processed. The decision also found that UCD had infringed Article 33(1) of the GDPR by failing to notify one of the personal data breaches to the DPC without undue delay. This personal data breach was notified 13 days after UCD became aware of it.

The decision ordered UCD to bring its processing operations concerning its email service into compliance with the infringed articles, reprimanded UCD in respect of its infringements, and imposed an administrative fine in the amount of €70,000 in respect of the infringements. UCD did not appeal against this decision. At the time of writing, the DPC is preparing its application to confirm the administrative fine.

Ryanair

In November 2020, the DPC adopted a decision concerning Ryanair. The complaint concerned cross-border processing in which the DPC was competent to act as lead supervisory authority. The decision found that Ryanair infringed Article 15 GDPR by failing to provide the complainant with a copy of a recording of a 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 decision also found that Ryanair infringed Article 12(3) GDPR by failing to provide the complainant information on action taken on their request under Article 15 within the statutory timeframe of one month. The decision reprimanded Ryanair in respect of the infringements. Case Study 10 of this report details this in full.

Groupon

In December 2020, the DPC adopted a decision concerning Groupon. The complaint concerned cross-border processing in which the DPC was competent to act as lead supervisory authority. The decision found that Groupon infringed Article 5(1)(c) GDPR by requiring the complainant to verify their identity by submitting a

copy of a national ID document. The requirement applied when data subjects made certain requests, but not when data subjects created a Groupon account, and a less data-driven solution to the question of identity verification was available to Groupon. The decision also found that Groupon infringed Articles 12(2), 17(1)(a) and 6(1) GDPR and reprimanded Groupon in respect of the infringements. Case Study 7 of this report details this in full.

Decisions under the Data Protection Acts 1988 and 2003

INM — December 2020

In addition to decisions made pursuant to the GDPR, the DPC continues to conclude a certain volume of complaints and investigations that must be decided according to the provisions of the Data Protection Acts 1988 and 2003. In December 2020, the DPC concluded an investigation into Independent News and Media (INM) and its compliance with its obligations as a data controller under the Data Protection Acts 1988 and 2003, with the Final Report having issued since to INM. The DPC's investigation was in connection with a data security incident which occurred in late 2014 and concerned the processing of personal data held in INM's internal IT and backup systems. The DPC found that INM contravened the Acts in a number of respects. The findings of infringement under the Data Protection Acts 1988 and 2003 relate to section 2(1)(a) and 2D (fairness and transparency of processing), 2A(1) (legal basis for the processing) and 2(1)(d) and 2C (security of processing of personal data).

Public Services Card

Appendix III of the DPC's 2019 Annual Report set out details of the investigation into the processing of personal data by DEASP in relation to the Public Services Card. Enforcement action was taken in December 2019 by the DPC in relation to that matter by the serving of an Enforcement Notice on the Minister for Employment Affairs and Social Protection. That Enforcement Notice was subsequently appealed by the Minister and these appeal proceedings remain ongoing before the Dublin Circuit Court.

Separately the DPC is continuing its investigation into certain other aspects of processing carried out by DEASP in connection with the issuing of PSCs and the SAFE 2 registration system, including the security of processing, facial matching processing by DEASP in connection with the PSC and specific use cases of the PSC.



6

Other Investigations and Enforcement Actions

Surveillance by the State Sector for Law Enforcement Purposes

Video surveillance systems that capture images of people and in turn lead to the identification of individuals, either directly or indirectly, (i.e. when combined with other pieces of information) can trigger the applicability of the GDPR and the Data Protection Act 2018. From a data protection perspective, video surveillance impacts the rights and freedoms of individuals significantly and it is therefore important that any such systems are operating in compliance with data protection law.

It was on this basis that in June 2018 the DPC commenced a number of own-volition inquiries under the Data Protection Act 2018 into video surveillance of citizens by the state sector for law-enforcement purposes through the use of technologies such as CCTV, body-worn cameras, drones and other technologies such as automatic number-plate recognition (ANPR) enabled systems. These own-volition inquiries are being conducted under Section 110 and Section 123 of the Data Protection Act 2018 using the data protection audit power provided for in Section 136 of the Data Protection Act 2018. The first phase of these inquiries are focusing on the use of video surveillance by the 31 local authorities in Ireland and also the use of video surveillance by An Garda Síochána. The purpose of these inquiries is to probe whether the data controllers of such systems can demonstrate that their systems are operating in compliance with data protection legislation.

Local Authorities

Since September 2018 the DPC has conducted inspections in the following local authorities: Kildare County Council, Limerick City and County Council, Galway County Council, Sligo County Council, Waterford City and County Council, Kerry County Council and South Dublin County Council. Between them, these seven local authorities have more than 1,500 CCTV cameras in operation for surveillance purposes. (The inquiries do not apply to security cameras such as those deployed for normal security purposes).

As part of the inquiry process, the DPC sought from the respective data controller's evidence of robust data protection policies as well as evidence of active oversight and meaningful governance. Weaknesses were identified in a number of local authorities that highlighted gaps in transparency. Concerns also emerged regarding the security of personal data collected through surveillance technologies.

Where live monitoring of CCTV systems occur, as opposed to accessing the footage on an incident basis, the DPC noted a failure by data controllers to demonstrate that the CCTV systems were being accessed or managed appropriately. Another common theme in the local authorities inspected was a lack of regular reporting on key metrics such as the number of times a system was accessed or the purpose for the access.

The type of CCTV devices used may also raise data protection concerns. Pan-Tilt -Zoom (PTZ) cameras may be used to zoom in from a considerable distance on individuals and their property and as such the processing

capabilities of these devices may pose higher risks to individuals' privacy. Furthermore, the deployment of automatic number-plate recognition cameras (ANPR) is becoming more common place in the State Sector but the absence of data protection policies governing the use of such technology is notable.

The inquiries in the local authority sector also involve auditing the deployment of community-based CCTV systems authorised under Section 38(3)(c) of the Garda Síochána Act 2005. These schemes require that the local authority be a data controller and that prior authorisation of the Garda Commissioner be obtained. The inquiries are examining, among other things, how data controller obligations are being met by the local authorities as required under that Act.

At the time of writing, the DPC has completed its inquiries in respect of six of the aforementioned local authorities and a final inquiry report for the seventh local authority is currently being finalised. While each of the local authorities inspected has its own unique approach to how it conducts surveillance on citizens, the DPC's work in this area has led to the identification of significant data protection compliance issues in relation to matters such as the use of covert CCTV cameras, the use of CCTV to detect illegal dumping, the use of body-worn cameras, dash-cams, drones and ANPR cameras, CCTV cameras at amenity walkways or cycle-tracks, and a lack of policies and data protection impact assessments. Equally, the DPC has significant concerns about how local authorities are discharging their data protection obligations as data controllers and the pressing need for them to do more to bring their operations into compliance with data protection legislation and to ensure accountability for the CCTV systems under their control.

Decisions

Of the various inquiries conducted by the DPC into the use of surveillance technologies by local authorities, the DPC has completed two inquiries — into Kerry County Council and Waterford City and County Council in relation to their use of video surveillance equipment, issuing final decisions in both. While Kerry County Council initially lodged an appeal against the DPC decision at the Circuit Court under Section 150 of the Data Protection Act 2018, this appeal was later withdrawn by the Council.

Further detailed information regarding these decisions can be found in Chapter 5 of this report.

An Garda Síochána

Separate to the ongoing inquiries in the local authority sector, an inquiry was conducted into An Garda Síochána in relation to Garda-operated CCTV schemes (Section 38(3)(a) of the Garda Síochána Act 2005 provides a legislative basis for such schemes).

Further detailed information regarding this inquiry and decision, which issued in August 2019, can be found in the published 'DPC Regulatory Activities Report May 2018 — May 2020' at Appendix 1: Surveillance by the State Sector for Law Enforcement Purposes.

Cookies Investigations Sweep and Enforcement

During the year the DPC considerably expanded our cookies investigations, examining a significant number of websites to assess compliance with the relevant legislation, i.e. Regulation 5(3), 5(4) and 5(5) of the ePrivacy Regulations (S.I. 336/2011). That legislation provides that consent must be obtained for placing any information on a user's device, or accessing information already stored on their device, unless one of two limited exemptions are met. It is important to note that the law applies not only to websites, but also to mobile apps and other products that use cookies or similar tracking technologies that access a device. The DPC's investigations into cookies was initiated against a backdrop of increasing public focus on the use of such technologies to track individuals across their devices and their online activity generally.

In April, the DPC published new guidance in relation to the use of cookies and tracking technologies. This was produced following a cookies sweep carried out in relation to 40 websites between August 2019 and December 2019. A report of that exercise was published along with the guidance.

Organisations were given a six-month deadline within which to bring their websites and other services using cookies into compliance. During that period the DPC conducted an extensive public awareness campaign in relation to the new, signalling its intention to begin follow-up enforcement action during Q4 of 2020.

Arising from its cookies investigations, on 27 November 2020, the DPC wrote to 18 organisations and to a further two organisations on 14 December 2020, about non-compliance issues on their websites, warning of the DPC's intention to issue Enforcement Notices without further notice, if these issues of non-compliance were not addressed within 14 days. These letters were effective in bringing several organisations substantially into compliance or into full compliance without the need for further enforcement action by the DPC. However, the DPC will continue to monitor the current state of compliance on an ongoing basis by all organisations who have been contacted by the DPC in relation to their use of cookies.

Some organisations failed to take sufficient remedial steps to bring their websites into compliance within the 14-day period that the DPC had set out in its letters to them. As a result, on 21 December 2020, the DPC served Enforcement Notices on seven organisations for non-compliance. The notices were issued pursuant to Regulation 17(4) of the ePrivacy Regulations (S.I. 336/2011) for infringements of Regulation 5, including failure to obtain valid consent for the use of cookies and for failing to provide clear and comprehensive information about the use of cookies on the websites concerned.

It was also notable during 2020 that the DPC began seeing more complaints and concerns from members of the public about the use of cookies and tracking technologies and it is expected that this trend will continue.

Investigations and enforcement in this area will continue to be a key element of the DPC's activities in 2021 and beyond.

The background of the page features a close-up, slightly blurred image of a pair of metal scales of justice. The scales are made of dark, possibly bronze or steel, metal. The chains are thick and made of interlocking links. The pans are shallow and circular. In the foreground, the left pan is visible, hanging from a chain. In the background, the right pan is visible, also hanging from a chain. The scales are set against a light, neutral background. Overlaid on the right side of the page are several abstract green graphics. These include concentric circles of varying sizes, some solid green circles, and a sunburst-like shape with radiating lines. The colors are a vibrant lime green. The overall design is modern and professional, suggesting themes of law, justice, and balance.

7

Legal Affairs

No.	Record No.	Title	Type of action and Venue	Date of Judgment/Order
1.	2018/4097	The Courts Service v. DPC (Notice Party: PM)	Statutory appeal Circuit Court	6 February 2020
Outcome:			Current Status of Case:	
<p>By decision dated 13 June 2018, made under the Data Protection Acts, 1988 and 2003 ("the DP Acts"), the Data Protection Commissioner held that, by publishing a judgment identifying the Notice Party by name, in circumstances where the High Court had earlier directed that the Notice Party's name should not be published, the Courts Service (1) failed to discharge its obligation to take appropriate security measures against unauthorised disclosure of the Notice Party's personal data, contrary to Section 2(1)(d) of the DP Acts; (2) processed the Notice Party's personal data (and sensitive personal data) without a lawful basis under Sections 2A and 2B of the DP Acts.</p> <p>By judgment pronounced on 6 February 2020, the Circuit Court refused an appeal by the Court Service, the Courts Service having sought orders setting aside the judgment and the DPC's determination that the Courts Service was a "data controller" for the purposes of the DP Acts.</p> <p>The Circuit Court did, however, limit the time period referable to the Courts Service's breaches of Sections 2A and 2B of the DP Acts to the period 12 May 2014 to 15 May 2014. The Court also set aside the DPC's finding that the Courts Service had failed to discharge its (security) obligations under Section 2(1)(d) of the DP Acts.</p> <p>No costs were ordered as between the Courts Service and the DPC. The Courts Service was directed to pay two-thirds of the Notice Party's costs with the balance to be paid by the DPC.</p> <p>Note that reporting restrictions put in place by Order of Judge Linnane dated 26 November 2018 in relation to the identity of the Notice Party remain in force by order of the High Court.</p>			<p>The Judgment and Order of the Circuit Court is the subject of an appeal to the High Court on certain points of law, brought by The Courts Service.</p> <p>Separately, the DPC has also applied to vary the Judgment and Order of the Circuit Court insofar as the Circuit Court allowed the appeal in relation to Section 2(1)(d) of the DP Acts and imposed a temporal limitation on the Courts Services' breach of Sections 2A and 2B. The DPC is also appealing against the Circuit Court's orders for costs.</p>	
2.	2019/211 CA	Doolin v. DPC (Notice Party: Our Lady's Hospice and Care Services)	Statutory appeal High Court	21 February 2020
Outcome:			Current Status of Case:	
<p>The High Court allowed an appeal on a point of law against an earlier decision of the Circuit Court (1 May 2019) in which the Circuit Court had in turn upheld a statutory decision of the Data Protection Commissioner made under Section 10 of the Data Protection Acts, 1988 and 2003.</p> <p>The High Court held that a finding made by the Circuit Court to the effect that the use of material derived from CCTV footage in the context of a disciplinary hearing amounted to processing for security purposes could not be sustained on the evidence. Accordingly, the DPC had made an error of law in holding that no further processing of the Applicant's personal data took place when material derived from the footage in question was deployed by the Applicant's employer in the course of a disciplinary hearing, such material having been obtained for a different purpose, i.e. a purpose relating to security.</p>			<p>The Judgment and Order of the High Court is the subject of a further appeal to the Court of Appeal; that appeal is listed for hearing on 26 June 2021.</p>	
3.	2019/564 JR	Department of Employment Affairs & Social Protection v. DPC	Judicial Review High Court	3 March 2020 (Final Order)
Outcome:			Current Status of Case:	
<p>On consent, the High Court quashed a decision of the DPC made on 5 June 2019 in which the DPC had upheld a complaint made by a named individual in respect of the lawfulness of the Department's processing of personal data relating to child benefit payments.</p>			<p>Proceedings complete.</p>	

No.	Record No.	Title	Type of action and Venue	Date of Judgment/Order
4.	2019/5078	Department of Employment Affairs & Social Protection v. DPC	Statutory appeal Dublin Circuit Court	5 March 2020 (Final Order)
Outcome:			Current Status of Case:	
On consent, an appeal brought by the Department against a decision of the DPC made on 5 June 2019 [the same decision as referred to above] was struck out, with no order for costs, in circumstances where, on foot of separate judicial review proceedings brought by the Department, the decision in question was quashed by order made by the High Court, on consent, on 3 March 2020 (see entry at item 3 above).			Proceedings discontinued.	
5.	2020/305 JR	Consumentenbond & others v. DPC	Judicial Review High Court	29 June 2020 (Final Order)
Outcome:			Current Status of Case:	
On 1 May 2020, the Applicants applied to the High Court by way of judicial review to seek certain orders in relation to the conduct on an ongoing statutory inquiry being undertaken by the DPC into the processing of location data by Google. Certain terms having been agreed between the parties, the proceedings were struck out, on consent, on 29 June 2020. No order for costs was made.			Proceedings discontinued.	
6.	2018/139	Nowak v. DPC (Notice Party: PWC)	Statutory appeal Court of Appeal	1 July 2020 (Written Judgment)
Outcome:			Current Status of Case:	
The Court of Appeal delivered a written judgment on 1 July 2020 , refusing an appeal by Mr Nowak against an earlier judgment of the High Court in which the High Court had upheld a decision of the DPC to the effect that certain memoranda held by PWC did not contain personal data relating to Mr Nowak and so Mr Nowak was not entitled to exercise a right of access to same.			Proceedings concluded.	
Subsequent to its judgment, the Court of Appeal delivered a written ruling on 27 July 2020 on the issue of costs, holding that Mr Nowak must pay the DPC's costs of the appeal before the Court of Appeal and also the costs of the courts below.				
Separately, Mr Nowak applied to the Supreme Court for leave to bring a further appeal to that Court. That application was refused by written determination made by the Supreme Court on 16 December 2020 .				
7.	2018/140	Nowak v. DPC (Notice Party: Chartered Accountancy Ireland)	Statutory appeal Court of Appeal	1 July 2020 (Written Judgment)
Outcome:			Current Status of Case:	
The Court of Appeal delivered a written judgment on 1 July 2020, refusing an appeal by Mr Nowak against an earlier judgment of the High Court in which the High Court had upheld a decision of the DPC to the effect that, in the context of a subject access request, Mr Nowak was entitled to obtain a copy only of his personal data, Mr Nowak having asserted that he was entitled to access his personal data in its original or raw form.			Proceedings concluded.	
Subsequent to its judgment, the Court of Appeal delivered a written ruling on 27 July 2020 on the issue of costs, holding that Mr Nowak must pay the DPC's costs of the appeal before the Court of Appeal. No order was made in respect of the costs of the courts below.				
Separately, Mr Nowak applied to the Supreme Court for leave to bring a further appeal to that Court. That application was refused by written determination made by the Supreme Court on 16 December 2020 .				

No.	Record No.	Title	Type of action and Venue	Date of Judgment/Order
8.	C-311/18	DPC v. Facebook Ireland Limited & Schrems	Preliminary reference from the Irish High Court CJEU	16 July 2020 (Written judgment)

Outcome:

The Court of Justice of the European Union delivered judgment on 16 July 2020, in which it addressed 11 questions posed by the Irish High Court in the context of a preliminary reference made on 4 May 2018.

In summary, the CJEU upheld the validity of a decision of the EU Commission incorporating the “standard contractual clauses” mechanism by which personal data may be lawfully transferred from the EU/EEA to a third country in respect of which an adequacy decision has not been adopted by the EU Commission.

Importantly, the CJEU went on to clarify the nature and extent of the obligations to which data exporters and supervisory authorities are subject in any case where SCCs are relied on to justify data transfers to a third country, with a view to ensuring that, in terms of appropriate safeguards, enforceable rights and effective legal remedies, data subjects whose personal data are transferred to a third country are afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR, read in the light of the Charter.

Having made certain findings of general application relating to the adequacy of the protection provided to EU citizens in the United States, the CJEU also ruled that the EU Commission’s decision adopting the “Privacy Shield” arrangements for data transfers to US was invalid.

Note that the issue of costs in the underlying proceedings was the subject of a separate ruling by the High Court made on 28 October 2020, referred to at item 12 below.

See detailed description of these proceedings in the Appendix V

Current Status of Case:

Proceedings complete.

9.	2020/5	Scott v. DPC	Appeal against order made in judicial review Court of Appeal	31 July 2020 (Final Order)
----	--------	---------------------	---	-------------------------------

Outcome:

By written judgment of 5 December 2019, the High Court struck out judicial review proceedings brought by Ms Scott under High Court Record No. 2019/95 JR. The proceedings were struck out on grounds of mootness, on the application of the DPC, the DPC having earlier delivered decisions in respect of certain complaints filed by the Applicant. (In her judicial review proceedings, Ms Scott had sought orders compelling the delivery of decisions in respect of her complaints).

On 3 January 2020, Ms Scott filed an appeal against Judgment and Order of the High Court.

Ultimately, Ms Scott agreed to withdraw that appeal. It was duly struck out, on consent, on 31 July 2020.

Note that one of the two decisions delivered by the DPC referred to above is presently the subject of a (separate) statutory appeal brought by Ms Scott in Dublin Circuit Court. That appeal has not yet come on for hearing.

Current Status of Case:

Proceedings complete.

No.	Record No.	Title	Type of action and Venue	Date of Judgment/Order
10.	2020/00172	Kerry County Council v. DPC	Statutory appeal Kerry Circuit Court	10 September 2020 (Final Order)
Outcome:			Current Status of Case:	
An appeal brought by Kerry County Council against a decision of the Commission made on 3 March 2020 following an inquiry under the Data Protection Act 2018 (concerning the deployment of CCTV by the Council in particular contexts) was withdrawn, without having been heard. No order for costs was made.			Appeal discontinued.	
11.	2017/464 CA 2017/459 CA	Grant Thornton Corporate Finance v. Scanlan	Appeal against order made in plenary action Court of Appeal / Supreme Court	28 September 2020 (Final Order)
Outcome:			Current Status of Case:	
On 31 October 2019, the Court of Appeal dismissed an appeal by the Defendant, Ms Scanlan, against an earlier order of the High Court refusing Ms Scanlan's interlocutory application to join the DPC to these proceedings. (The proceedings are concerned with Ms Scanlan's refusal to take certain steps in respect of information received by her from Grant Thornton relating to identifiable third parties).			Proceedings complete.	
Ms Scanlan's subsequent application for leave to bring a further appeal to the Supreme Court was refused by the Supreme Court by written determination made on 31 September 2020.				
12.	2019/718 JR	Scott v. DPC	Judicial review High Court	13 October 2020 (Final Order)
Outcome:			Current Status of Case:	
By Order of 13 October 2020, made with the consent of the parties, the High Court struck out judicial review proceedings brought by Ms Scott under High Court Record No. 2019/718 JR, the DPC having earlier delivered a decision in respect of a particular complaint filed by the Applicant. (In her judicial review proceedings, Ms Scott sought an order compelling the delivery of the decision in question).			Proceedings complete.	
Costs were awarded to Ms Scott.				
The decision delivered by the DPC is presently the subject of a (separate) statutory appeal brought by Ms Scott in Dublin Circuit Court. That appeal has not yet come on for hearing.				
13.	2016/4809P	DPC v. Facebook Ireland Limited & Schrems	Plenary action seeking a preliminary reference to the CJEU High Court	28 October 2020 (Written ruling)
Outcome:			Current Status of Case:	
Following written and oral submissions by the parties, the High Court made a ruling on 28 October 2020 directing the DPC to pay Mr Schrems' costs of the proceedings in the High Court and CJEU.			The final order has not yet been perfected and so the time-period for the bringing of an appeal (if any) has not yet expired.	
The High Court refused the DPC's application for an order directing Facebook to pay the DPC's costs and to bear responsibility for such costs as the DPC was ordered to pay to Mr Schrems.				

No.	Record No.	Title	Type of action and Venue	Date of Judgment/Order
14.	2020/02845	DPC v. Tusla/Child & Family Agency	Statutory application Dublin Circuit Court	4 November 2020 (Final Order)

Outcome:

On the application of the DPC, an order was made by the Circuit Court pursuant to section 143(2) of the Data Protection Act 2018, confirming an administrative fine levied by the DPC on Tusla (in the sum of €75,000) pursuant to a decision of the DPC dated 7 April 2020 following an inquiry under the Data Protection Act 2018. Costs were also awarded to the DPC.

Current Status of Case:

Application completed.



8

Supervision

Engagement with public and private sector organisations, policy makers and legislators enables the DPC to understand the ways in which personal data are being processed by data controllers and processors, and enables the DPC to proactively identify data protection concerns and, in the case of new products or services to ensure that organisations are aware of their compliance obligations and potential problems in advance of the commencement of the processing of personal data.

The aim of supervision engagement is to offer guidance to stakeholders and to connect proactively as a regulator with a visible presence, ensuring the data protection rights of service users are upheld. In this way, the DPC advocates for the rights of individuals by mitigating against potential infringements before they occur. The Supervision function is an important part of the regulatory framework, as ensuring best practice is applied at project planning stages results in better outcomes for data subjects and less need for resource-intensive ex-post activity for the DPC.

The DPC received 724 consultation requests during 2020. The sectoral breakdown is as follows:

Sector	#	%
Private Sector	413	57%
Public Sector	191	26%
Health Sector	89	13%
Voluntary/Charity Sector	23	3%
Law Enforcement Sector	8	1%
Total	724	

Health Sector

The DPC began the year with attendance at grand rounds in several major hospitals, working with Data Protection Officers to bring practical advice and guidance to frontline healthcare staff. While this outreach work was curtailed by the Covid-19 pandemic, it is intended to resume this very successful programme when possible in 2021.

Covid-19

2020 has been an extraordinary and challenging year due to the Covid-19 pandemic. The DPC was involved from an early stage in working to assist organisations in understanding the data protection implications of the many measures that they were asked to undertake to combat the spread of the virus. The DPC also engaged with Government Departments to ensure that data protection was given appropriate consideration in the development of public policy and legislation in the context of the pandemic.

The DPC published guidance and blog pieces on a range of topics affected by Covid-19, including Processing Customer Data for Covid-19 Contact Tracing, the Data Protection Implications of the Return to Work Safely Protocol, and Protecting Personal Data When Working Remotely.

In the areas of public health policy and legislation, the DPC engaged with Government in relation to such areas as the national Return to Work Safely Protocol and the Covid-19 Passenger Locator Form. The DPC has also engaged with the HSE on the data protection implications of contact tracing.

Given the global nature of the Covid-19 pandemic, the DPC also engaged with international partners to assist in addressing the data protection implications in a consistent manner. This included participation in the work of the European Data Protection Board, joining the Global Privacy Assembly's Covid taskforce, and working directly with colleagues at the UK Information Commissioner's Office. The DPC will continue to work with global partners in 2021 to ensure that we can give accurate best practice advice to organisations in Ireland, in particular looking at the processing of personal data relating to vaccinations and vaccine programmes.

Covid19 Contact Tracing App

At an early stage in the global spread of the Covid-19 virus, it was recognised internationally that mobile phone apps might be used to assist in contact tracing efforts. In March 2020, the DPC commenced a consultative engagement with Government stakeholders on the possibility of the development of a national contact-tracing app. The DPC emphasised the significant data protection challenges arising from any use of location data, in particular, and the need for the Government to incorporate data protection concerns at the earliest stage in the project.

In parallel to discussions with the national app project stakeholders, the DPC also engaged in research and in

discussions with international colleagues to gain a fuller understanding of the data protection implications of this emerging and rapidly developing technological solution. This included reaching out to Google and Apple, the joint developers of the Bluetooth-based Exposure Notification System on which the Irish app would be based.

The first phase of the consultative process on the app ended with the provision by the DPC of an in-depth report on the Data Protection Impact Assessment (DPIA) for the Covid Tracker Ireland app. In examining this DPIA, the DPC wanted to ensure that before an app was launched for use by the Irish public, all data protection risks had been adequately assessed and accounted for. The DPIA was also assessed in light of the published guidance of the EDPB on the use of location data and contact tracing tools. In the interests of transparency, the DPC recommended the publication of the DPIA and all ancillary documentation to allow full public scrutiny.

Following the launch of the Covid Tracker Ireland app, the DPC has continued to engage with the Department of Health and other stakeholders on the implementation of cross-border app interoperability and on the monitoring of the application of safeguards to protect the personal data undergoing processing.

Genomics

In 2020, as part of its ongoing work with the health research sector, the DPC engaged in a supervision exercise with Genuity Science (Ireland) Ltd, to review the company's data protection compliance measures and where necessary to seek the implementation of remedial action. This included looking at systems for consent management and the withdrawal of consent by research participants, as well as clarifying the conditions for third party access to research data. In 2021, the DPC will continue this engagement, seeking the implementation of recommendations put forward in its initial phase.

In the developing area of genomics, and in the wider life sciences, the DPC takes a proactive role in working with industry and researchers to ensure that important healthcare outcomes are delivered in a manner that respects the data protection rights of individuals. As part of this strategy, the DPC has also engaged with industry groups in the medical device, and cell and gene therapy areas, as well as working with our European colleagues on questions regarding the application of GDPR to scientific research.

Public Sector

In addition to engagement with Government and public bodies on matters relating to Covid-19, the DPC provided guidance on a range of legislative and public policy measures in 2020. Since the introduction of GDPR and the Data Protection Act 2018, the DPC has worked to develop relationships with key decision-makers in public bodies to facilitate early engagement on legislative proposals and policy initiatives and this continued in 2020. This foregrounding of data protection concerns ensures respect for the principle of data protection by

design and is in the best interests of upholding the data protection rights of Irish citizens.

Sample of legislative consultations:

- Health Act 1947 (Section 31A — Temporary Requirements) (Covid-19 Passenger Locator Form) Regulations 2020.
- Health Act 1947 (Section 31A — Temporary Restrictions) (Covid-19) (No. 4) Regulations 2020.
- Road Traffic (Licensing of Drivers) (Amendment) (No. 8) Regulations 2020
- Forestry (Miscellaneous Provisions) Act 2020
- Transposition of Directive (EU) 2019/770 on contracts for the supply of digital content and digital services
- Garda Síochána (Digital Recording) Bill — General Scheme
- Preservation and Transfer of Specified Records of the Commission of Investigation (Mother and Baby Homes and certain related Matters) Bill
- Higher Education Commission Bill 2020
- Transposition on 5th AML Directive and creation of beneficial ownership registers for (a) Trusts (b) Bank A/c's (c) Investment Vehicles & credit unions
- Finance Bill — Revenue Commissioners collection of aggregated credit card transactions from Financial institutions regarding VAT collection from online retailers
- Irish transposition of Directive 2018/1972 establishing the European Electronic Communications Code
- Certain Institutional Burials (Authorised Interventions) Bill

Sample of Non-Legislative Consultations

- Carrying out of Leaving Certificate 2020 and Calculated Grades System in the context of Covid-19
- Various public service data initiatives led by OGCIO, including Public Service Data Catalogue and Public Service Data Governance Board
- Online provision of national driver theory test
- Data sharing between the National Vehicle and Driver File (NVDF) and An Garda Síochána
- Conduct of Census 2021 by the CSO
- Voter.ie project, administered by Dublin City Council on behalf of Dublin City Council and Fingal, Dun Laoghaire Rathdown, South Dublin County Council
- Development of a national Motor Third Party Liability database
- Processing of equality data by public sector bodies for statistical purposes
- The Residential Tenancies Board tenancy Management system
- Processing of personal data by Owners Management Companies of Multi-Unit Developments, with the Housing Agency
- Multi-stakeholder consultation on electricity smart-metering
- Use of drones in waste enforcement by Local Authorities

Leaving Certificate 2020

The DPC proactively contacted the Department of Education and Skills over its plans for a revised Leaving Certificate 2020 due to the Covid-19 pandemic. The focus of our consultation with the Department was to ensure that the revised Leaving Cert was appropriately assessed from a data protection point of view and that processing of personal data was fair, lawful and conducted in a transparent manner during all stages of the process. The DPC was particularly concerned to ensure that there would be full transparency to students and external parties on the calculation of grades and the standardisation process, and that issues relating to students' access to their class rank were satisfactorily addressed by the Department. Whilst the DPC recognises that difficulties arose in respect of an error with the algorithm used to assess calculated grades, it was satisfied that the Department had met its obligations from the data protection viewpoint. The Department, by providing detailed information in relation to the processing and how grades were calculated allowed students, parents and teachers to assess and question the accuracy of the final calculated grades. Adequate information and subsequent scrutiny by the processor ultimately led to the identification of the much-publicised error in the algorithm which in turn saw over 6,000 students receive upgraded results. This highlights the significance of the role transparency can play in terms of meeting principles of fairness and in terms of being able to assess the accuracy of processing.

Financial & Private Sector

Anti-Money Laundering & Terrorist Financing Requirements

The requirements under the anti-money laundering and terrorist financing (AML) laws for controllers to process personal data of their customers, through a reasonable risk based approach, to detect or prevent AML, continues to be a challenging issue. During 2020 the DPC engaged with DPOs in the financial sector on concerns in the following areas:

- Excessive collection of customer data where it is not a relevant and necessary requirement under the AML laws;
- Excessive processing of customer financial data where there is no suspicion of illegal activity and enhanced due diligence measures are not necessarily required to be done; and
- Excessive automated profiling of customer databases with enforcement agencies watch lists.

Companies that process substantive amounts of customer data for AML compliance that they should have completed a DPIA which has assessed the risks to individuals related to the policies and procedures in place for AML processing.

New databases for AML Beneficial ownerships under the 4th & 5th AML Directives.

During 2020 the DPC engaged in extensive consultation on the establishment of the following databases:

- Registrar of Beneficial Ownership of Companies and Industrial & Provident Societies. Statutory Instrument No 110/2019 requires all corporate and legal entities to file adequate, accurate and current information on their beneficial owner(s);
- Central Bank's Beneficial Ownership Register is to deter Money Laundering and Terrorist Financing and to identify those that seek to hide their ownership and control of corporate or legal entities by ensuring that the ultimate owners/controllers of ICAVs, Credit Unions, Unit Trusts, are identified; and
- Register of the Beneficial Ownership of Trusts. The draft legislation is being prepared by the Department of Finance.

Smart Metering

In 2020 the DPC continued to engage with the stakeholders involved in the design and roll-out of Ireland's Smart Metering programme. In particular, the DPC advocated the need for greater transparency to the public and interested parties on how the protection of personal data is being addressed and the efforts made to eliminate or reduce any risk to data protection of individuals. The DPC welcomes the steps taken to enhance transparency which has included the publication of DPIAs by ESB Networks and updated guidance materials by the Commission for Regulation of Utilities (CRU).

Fintech Survey

During the first quarter of 2020, the DPC invited companies in the growing Fintech sector in Ireland to engage in a data protection survey. Questions were issued to controllers and processors covering topics such as Lawful Basis, Accountability, International Transfers and the Data Protection Rights of Individuals. Whilst the survey gave the DPC an opportunity to understand the level of data protection understanding within the industry, it also made the organisations aware of the availability of the DPC to assist in a consultative capacity on any of the questions posed.

Some findings from the survey include:

- 95% of respondent claimed to have trained employees on data protection requirements;
- 66% have engaged in the services of a Data Protection Officer and only 33% have registered a Data Protection Officer with the DPC;
- 33% of all respondents claimed to have carried out a Data Protection Impact Assessment relating to their processing of personal data and all respondents claim to have considered any data protection by design or default in its processing or technology systems;
- 40% transfer personal data outside of the EEA; and

- 66% of controllers collect personal data from publically available sources such as the Companies Registration Office or Tax Defaulters Lists whilst less than in one in four use social media or newspaper publications to collect personal non-analytical data.

TikTok Ireland and Main Establishment

During 2020, TikTok Ireland's declaration of main establishment in Ireland for the purpose of availing of the GDPR one-stop-shop was examined. In assessing whether TikTok Ireland had met the objective criteria of main establishment, the DPC reviewed detailed documentation and responses provided by TikTok setting out the legal, administrative, governance and other measures implemented. The question of main establishment was considered under the lens of Article 4(16) of the GDPR, Recital 36 of GDPR and the EDPB Guidelines for identifying a controller or processor's lead supervisory authority.

Some of the key issues considered were:

- Where are decisions about the purposes and means of the processing given final 'sign off'?
- Where are decisions about business activities that involve data processing made?
- Where does the power to have decisions implemented effectively lie?
- Where is the Director (or Directors) with overall management responsibility for the cross border processing located?
- Where is the controller or processor registered as a company, if in a single territory?

Based on its assessment of the measures implemented to satisfy the main establishment criteria, the DPC was ultimately satisfied that TikTok Ireland was in a position to demonstrate effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements.

Case Studies

Case Study 17:

Vodafone seeks employment details from customers

The DPC received a number of queries regarding new or existing customers being requested by Vodafone to produce their employment details and work phone number as a requirement for the provision of service by that company.

The concerns arising were that the requests were excessive and contrary to the Article 5 principle of lawful, fair and transparent collection as the processing of data relating to their employment status was entirely unrelated to the product or service that they were receiving from the telecommunications company, which was for their personal or domestic use only.

Second, there were concerns that the mandatory request for a customer's occupation/place of work/work phone number was not adequate,

relevant or necessary under the "data minimisation" requirement and did not meet the purpose limitation principle as set out in Article 5 of GDPR.

Third, there were also concerns amongst customers that the company's data protection/privacy notice did not comply with the transparency requirement of GDPR Article 13(1).

Following engagement with the DPC, Vodafone admitted that it had made an error in the collection of this information. The company stated that the problems were caused by a legacy IT system that had not been updated to remove this requirement and that any access to the data was exceptionally limited and was not used for any additional processing purposes by them. Vodafone immediately commenced a plan to remediate the problems caused and, on the insistence of the DPC, published on its website the details of what had occurred, so that customers would be aware of the issue.

Case Study 18:

Facebook Dating

In February 2020, the DPC was informed of Facebook's impending launch of 'Facebook Dating' in the EU. A cause for significant concern was the short notice given about its launch, together with very limited information on how Facebook had ensured the Dating feature would comply with data protection requirements. As a result, the DPC undertook an on-site inspection of

Facebook's offices in Dublin to obtain more extensive documentation and information. A number of queries and concerns identified by the DPC were put to Facebook on the new product and its features. 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.

These changes included:

- clarification on the uses of special category data which was very unclear in the original proposal. Facebook agreed that there would be no advertising using special category data and special category data collected in the dating feature will not be used by the core Facebook service;
- changes to the user interface around a user's selection of religious belief so that the "prefer not to say" option was moved to the top of the list of options;
- greater transparency to users by making it clear in sign-up flow that Dating is a Facebook product and that it is covered by Facebook's terms of service and data policy and the Supplemental Facebook Dating Terms; and
- revisions to the consent header for the processing of special category data to specifically flag that special category data (in this instance sexual preference and religious belief) will not be processed for the purposes of advertising (targeted or otherwise).

Case study 19:

Facebook Suicide and Self-Injury feature

In early 2019 the DPC was initially approached by Facebook and informed of their plans to implement an expansion of its Suicide and Self Injury Prevention Tool (SSI), which involved using advanced algorithms to monitor Facebook and Instagram users' online interactions and posts. Facebook intended that the tool would help identify users at risk of suicide or self-harm. Details of these users would then be notified to external parties (police and voluntary organisations) to action an intervention with the users concerned. The DPC raised a number of concerns during the engagement (2019–2020) including lawful basis and adequate safeguards relating to the processing of special category data. Facebook took the position that the processing of this data would rely on the public interest exemption under Article 9 GDPR.

As part of the DPC assessment it was suggested that Facebook should consult public health authorities in Europe before proceeding. Facebook acknowledged that they had further work to do and would undertake the consultation and further research with public health authorities across Europe on the SSI tool. Facebook has indicated that this engagement will continue to be a long-term initiative given the challenges experienced by Member State Governments and national public health authorities due to the Covid-19 pandemic. The DPC understands this engagement is ongoing.

In late 2020, Facebook approached the DPC proposing a more limited use of this tool for the sole purpose of removing content contravening Facebook Community Standards and Instagram Community Guidelines, pending resolution of the concerns raised by the DPC. No significant concerns were identified by the DPC so long as the processing was for the sole purpose of content moderation.

Case study 20:

Facebook Election Day Reminder

In advance of the Irish General Election in February 2020 the DPC notified Facebook that the Facebook Election Day Reminder (EDR) 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.

The DPC requested that Facebook implement a mechanism at the point at which users engage (or will engage) with the EDR function to ensure that the information referenced in Article 13 of the GDPR, including information addressing the specific

circumstances and context in which the processing operations are undertaken, be made available to users in an easily accessible form before a user decides whether or not to interact/engage with the EDR function. Of particular concern to the DPC was the lack of clarity from Facebook on whether any data generated by a user interacting with the feature would be used for targeted advertising and newsfeed personalisation.

As it was not possible to implement changes in advance of the Irish election, Facebook responded to the DPC advising that it intended to withdraw the roll-out of the EDR function for the election and that the feature would not be activated during any EU elections pending a response to the DPC which addressed the concerns raised.

Case study 21:

Google Voice Assistant Technology

The DPC engagement with Google on the company's voice assistant product continued in 2020. This engagement commenced following media coverage in the summer of 2019. 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.

These include:

- A new transparent user engagement and consent flow to include information about the suite of safeguards in place to minimise the risks

to data subjects and make user controls more accessible;

- Measures to decrease misactivations. Users can now adjust how sensitive Google Assistant devices are to prompts like "Hey Google," giving users more control to reduce unintentional activations, or to make it easier for users to get help in noisy environments. Google is also continuing to improve device and server side measures to detect false activations of Google assistant;
- Deletion by voice command on Assistant. Users are now able to delete their Assistant interactions from their account by saying things like "Hey Google, delete the last thing I said" or "Hey Google, delete everything I said to you last week." If users ask to delete more than a week's worth of interactions from their account, the Assistant will direct them to the page in their account settings to complete the deletion.





9

Data Protection Officers

DPO Notifications to the DPC

One of the tasks of the DPC is to maintain and update a Data Protection Officer (DPO) Register within the DPC, as notified to it by its relevant regulated entities, meaning those organisations who meet the threshold for DPO requirement.⁵

Article 37.7 of the GDPR states that “the controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.”

In 2020, the DPC received 517 DPO notifications through the online web-form on the DPC website. In total, the DPC’s DPO notifications database contains 2,166 records of DPOs. The table below shows the industry sectors from which notifications were made in 2020.

DPO notifications for 2020	
Private	417
Public	109
Non-for-Profit	44
Total in 2020	570 (2,166 overall)

Public Sector DPO Compliance

Article 37.1 of the GDPR stipulates, that all organisations that process personal data, either as a data controller or data processor, must designate a DPO where the ‘processing is carried out by a public authority or body’.

Article 37.7 of the GDPR states that “the controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.”

In 2020, the DPC commenced a project to assess compliance by public bodies with the Article 37 obligations. From a total of almost 250 public bodies, comprising Government Departments and agencies, as well as Local Authorities, 77 public bodies were identified as being potentially not compliant with the requirements. Engagement with each of these public bodies resulted in 66 bringing themselves in to compliance with Article 37.7 of the GDPR by the end of 2020, raising the sector’s compliance rate from 69% to 96%.

The DPC will continue to engage with the public sector bodies as required in 2021 to achieve compliance with GDPR Article 37(3).

The DPC has observed that some agencies of Departments have relied on Article 37(3) of the GDPR

which states that “Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size”.

A single DPO may be designated for several such authorities or bodies; however, this should not remove the obligation of that agency or business unit under a parent department to separately publish the contact details of their DPO and to separately communicate those details to the supervisory authority even if the parent department has also done so.

If a public body wishes to communicate details of a DPO, whether updating or registering a new DPO, this should be done through official channels using the DPC’s web-form or email.

The DPC will expand its compliance and monitoring activities in this area to include organisations other than public bodies that are also required to designate a DPO and comply with Article 37.7 of the GDPR during 2021. This will be conducted on a sector by sector approach. Organisations without a DPO are encouraged to consider whether they are required to have a DPO — further information is available on the DPC’s website.

Engagement with DPOs

The DPC remains committed to supporting DPOs and their teams, in recognition of the key role played by DPOs in ensuring that GDPR programmes translate into lasting organisational culture and compliance. DPC staff spoke at many virtual events for DPOs during the year. As part of the DPC’s efforts to empower DPOs in the conduct of their duties, the DPC established a DPO Network in late 2019. The purpose of the Network is to foster peer-to-peer engagement and knowledge-sharing between DPOs and data protection professionals.

Due to Covid-19, the planned DPC DPO Network Conference that was due to take place in March was necessarily postponed. The DPC has instead taken these supports online, with a dedicated section for DPOs on its website where the resources, including podcasts and guidance, are centralised for ease of access. The DPC continues to engage with DPOs on an ongoing basis, including a quarterly newsletter, to ensure that the resources it produces are informed by the needs of the cohort.

Codes of Conduct

During 2020 the DPC drafted accreditation requirements that potential Monitoring Bodies for Codes of Conduct were required to meet. ‘The Accreditation Requirements for Code Monitoring Bodies’ was approved by the EDPB and adopted by the DPC. This marked the final step in enabling the DPC to progress the establishment and approval of Codes of Conduct in Ireland in line with Articles 40 and 41 of the GDPR. The DPC is already engaged with several potential Code owners and anticipates receiving the first official draft Code early in 2021.

⁵ A DPO is mandatory for: Public authorities; Organisations whose core activities consist of processing operations that require regular and systematic monitoring of data subjects on a large scale; or Organisations whose core activities consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.



10

International Activities

International Transfers — Binding Corporate Rules

A key focus in the area of international transfers for the DPC is the assessment and approval of Binding Corporate Rules applications from multi-national companies.

Binding Corporate Rules (BCR) were introduced in response to the needs of organisations to have a global approach to data protection where many organisations consisted of several subsidiaries located around the globe, transferring data on a large scale. During 2020, the DPC continued to act or commenced acting as lead reviewer in relation to 42 BCR applications from 28 different companies. The DPC also assisted other European Data Protection Agencies (DPAs) by acting as co-reviewer or on drafting teams for Article 64 Opinions on 5 BCRs in this period.

The EDPB issued Article 64 opinions on nine BCR applications in 2020, including Opinions on the BCR-controller and BCR-processor of Reinsurance Group of America, for which DPC was lead authority.

Due to the departure of the UK from the EU in 2020, the DPC has had contact from a number of companies enquiring about transferring their lead authority for BCR purposes to the DPC. This process has been completed for a number of applicants, greatly increasing the DPC's workload in 2020.

Brexit

In the latter part of 2020 in the run up to the end of the Transition Period on 31 December, there was a very real possibility that the UK would finally depart without a deal with the EU and therefore fall outside EU data free-flows. This created implications for large sectors of Irish business and the public sector, who needed to put in place transfer mechanisms to allow for the continuance of legitimate transfers to the UK in the event of a no-deal Brexit.

The DPC maintained ongoing engagement with impacted stakeholders, to facilitate the prompt sharing of information throughout the evolution of the negotiation process.

On 24 December 2020, the Trade and Cooperation Agreement was signed and this agreement provided for data transfers, allowing for up to a six month period (the so called bridging period) whereby transfers to the UK could continue as if the UK was still part of the EEA, while negotiations on an adequacy agreement continue.

Other International Transfer Issues

In July 2020 the CJEU invalidated the Privacy Shield mechanism that had facilitated certain transfers from the EEA to the US and, while it upheld the use of Standard Contractual Clauses, it did make clear that if the laws and practices in a third country mean that the level of protection for data transferred there is not assured in a

given case, transfers would have to stop unless supplementary measures could plug any gaps in protection.

Draft recommendations on Supplementary Measures were published by the EDPB and submissions received on the draft are now being assessed by EDPB. A full note on the Litigation concerning Standard Contractual Clauses is available in Appendix 5 of this report.

European Data Protection Supervisory Authorities

During 2020, the DPC continued to participate in the work programmes of the European Supervisory Bodies for large-scale EU IT systems such as Europol, Eurodac, Eurojust, the Customs Information System (CIS) and the Internal Market Information (IMI) system. The DPC conducted a number of desk audits with the Europol National Unit in An Garda Síochána in relation to data subject rights and the processing of data in Europol systems. In addition, the DPC continued in its role as observer to the coordinated supervision of the Schengen and Visa Information Systems (SIS II and VIS). With regard to SIS II, the work programme to progress Ireland's participation will continue in 2021.

Consistency Mechanism and EDPB Tasks

Like all other EEA data protection supervisory authorities, the DPC must ensure that it interprets, supervises and enforces the GDPR in a way that achieves consistency. In 2020, the DPC participated in over 180 EDPB meetings (most of which were conducted virtually), including those of the 12 EDPB expert subgroups.

DPC staff members have contributed extensively to the development of guidelines and opinions across all of the EDPB expert subgroups during 2020. The DPC also acts as co-coordinator of the Social Media expert subgroup.

BIIDPA 2020

On 18 June 2020 the DPC hosted a virtual meeting of the British, Irish and Islands' Data Protection Authorities (BIIDPA) welcoming representatives from the supervisory authorities of Bermuda, the Cayman Islands, Gibraltar, Guernsey, the Isle of Man, Jersey, Malta and the UK. BIIDPA attendees share a common law background and meet each year to discuss a variety of data protection related topics. Issues discussed included Covid-19 and the DPC's Communications Strategy.

13-15 October Global Privacy Assembly

In October 2020 the DPC participated in the Global Privacy Assembly (GPA); the annual gathering of more than 130 data protection and privacy authorities from around the world.



11

Key DPC Projects

Children's Policy

Activities during 2020

Following the conclusion of the DPC's public consultation and the subsequent publication of two statistical reports on feedback from both the adult and child focused streams of the consultation in 2019, the DPC commenced the extensive process of drafting guidance for organisations that process children's data.

In tandem with this work, the DPC engaged with a number of child's rights experts and advocates from the public, private and non-profit sectors in order to seek further views in relation to various technical issues to be addressed in the guidance.

Throughout 2020, the DPC continued its participation as a member of the National Advisory Council for Online Safety, where it contributed to the Council's scrutiny of the General Scheme of the Online Safety and Media Regulation Bill — finalised by the Department of Tourism, Arts, Culture, Gaeltacht, Sport and Media in December 2020 — in order to ensure a clear framework for cooperation between the DPC and other regulators whose remits touch upon online safety concerns.

The "Fundamentals"

In December 2020, the DPC published its much-anticipated guidance document entitled "Children Front and Centre: Fundamentals for a Child-Oriented Approach to Data Processing" (the "Fundamentals" for short).

The Fundamentals address core data protection issues such as the age at which children can exercise their own data protection rights for themselves, the role of parents/guardians in acting on behalf of their children, age verification and verification of parental consent, as well as the rules governing the processing of children's personal data for direct marketing, profiling or advertising purposes.

The DPC also sets out in the Fundamentals a variety of recommended measures that will enhance the level of protection afforded to children against the data processing risks posed to them by their use of or access to services in both an online and offline world. The DPC is conducting a public consultation on the draft version of the Fundamentals and is inviting submissions from all interested parties until 31 March 2021.

Taking into account the feedback received, the DPC will publish the finalised version of the Fundamentals which will inform the DPC's enforcement, supervision and regulatory activities.

Codes of Conduct

During 2021, the DPC will also work with industry, government and voluntary sector stakeholders and their representative bodies to encourage the drawing up of Codes of Conduct in relation to the processing of children's personal data, in accordance with Section 32 of the Irish Data Protection Act 2018. This Codes of Conduct project will be a core initiative for the DPC in 2021.

Regulatory Strategy

Work on the DPC's Regulatory Strategy continued in 2020 — with both internal and external stakeholder engagement — and the development of the strategy is now nearing its conclusion. The development of the DPC's Regulatory Strategy has been an iterative process, evolving in response to the needs of stakeholders and their feedback. In drafting the strategy, the DPC has given careful consideration as to how it can best deliver improved results for the maximum amount of people, in a regulatory landscape that is constantly evolving in response to legal and societal needs.

An integral part of the strategy development process in 2020 was the production and publication of the DPC's Two-Year Activity Report under the GDPR, which was an opportunity to take stock of the reality of regulating since May 2018 and identify the thematic issues and statistics which must be factored into the DPC's strategic plan for the future. The DPC's regulatory analysis in 2020 also involved two workshop cycles, the first focusing on a horizon scan for 2020 and the second concentrating on complaint-handling methodologies going forward.

The Arc Project

The DPC continued its partnership with the Croatian Data Protection Authority, AZOP, and Vrije University in Brussels on an EU-Funded project (The ARC Project) — specifically targeting SMEs — to increase compliance across the SME sector. Work on the project began in Q1 of 2020 and will run for a further two years. Through this engagement — which includes surveys, roadshows and conferences — the project intends to develop a more detailed understanding of the climate in which SMEs are operating and provide practical resources to support them in their compliance efforts.



12

Communications

Media engagement

The profile of, and the media interest in, the DPC continued to grow both nationally and internationally during 2020. Much of the media engagement stemmed from the DPC's inquiry and litigation work, including significant international media attention surrounding the DPC's draft decision in the Twitter International Company inquiry.

Direct Engagement

The DPC continued to directly engage with a variety of stakeholders during 2020, adapting to the constraints imposed by Covid-19. From March onwards, all conferences and events in which the DPC partook were virtual. The DPC contributed to almost 100 events in 2020.

Guidance, blogs and podcasts

The DPC continued to produce, update and disseminate comprehensive guidance on a wide variety of topics for both individuals and organisations. Almost 40 items of guidance were produced in 2020, covering a wide range of issues ranging from video conferencing to contact tracing.

Activity report

In June, the DPC published 'DPC Ireland 2018-2020: Regulatory Activity Under GDPR' — a two-year regulatory activities report providing a wider-angled lens through which to assess the work of the DPC since the implementation of the GDPR. The trends and patterns identified will have bearing on the DPC's regulatory considerations going forward.

Social media

In 2020, the DPC continued to grow its social media presence across Twitter, Instagram and LinkedIn, in support of its awareness-raising and communications activities. The combined followers across the three platforms has increased by over 8,000 during 2020, to almost 29,000. There was an organic reach of almost 2.8 million, with strong engagement across the board.

DPC Website

The DPC website (www.dataprotection.ie) was a particularly important resource for individuals and organisations throughout 2020. In November, the DPC launched a redesign of the website, making it easier for users to find and navigate information. The redesigned site also includes a dedicated section for Data Protection Officers.





13

Corporate Governance

DPC Funding and Staffing

The funding of the DPC by government has increased year-on-year from €1.7 million in 2013 to €16.9 million in 2020 (comprising €10.5 million in pay and €6.4 million in non-pay allocation).

The DPC continued to engage with the Public Appointments Service to recruit staff during 2020. The process of recruitment was impacted by Covid-19. The DPC had a staff complement of 145 at year end, with two recruitment competitions still ongoing on 31 December 2020. Further recruitment of staff, in addition to those successful in these two competitions, is a priority for the DPC in 2021.

Corporate Services and Facilities

While DPC offices remained largely closed — physically — due to Covid-19 restrictions, the DPC continued to maintain a skeleton staff to process incoming and outgoing postal correspondence and provide the logistical support necessary to facilitate effective remote working for DPC staff.

Corporate Governance

The DPC became its own Accounting Officer on 1 January 2020. Accordingly, the DPC's internal controls were monitored in accordance with the Code of Practice for the Governance of State Bodies. The DPC's required annual Statement on Internal Control for 2020 will be published on the DPC's website with its Financial Statement later in the year.

DPC Audit and Risk

In 2020 the DPC established an Audit and Risk Committee, in keeping with the Corporate Governance Standard for the Civil Service (2015), and the Code of Practice for the Governance of State Bodies (2016).

The members of the committee are:

- Conan McKenna (chairperson);
- Bride Rosney;
- Karen Kehily;
- Michael Horgan; and
- Graham Doyle (DPC).

Seven meetings of the Audit and Risk Committee were held in 2020.

Official Languages Act 2003

During 2020 the DPC prepared its fifth Language Scheme under the Official Languages Act 2003. The finalised scheme was subsequently confirmed by the Minister for Tourism, Culture, Heritage, Arts, Gaeltacht, Sport and Media, submitted to the office of An Coimisinéir Teanga, and published on the DPC website. The fifth Scheme commenced on 21 December 2020 and remains in effect for a period of three years.

Freedom of Information (FOI)

In 2020, the DPC received a total of 65 FOI requests. Eight were granted, three were partially granted and 38 were deemed out of scope. The DPC's regulatory activity is exempted from FOI requests in order to preserve the confidentiality of our supervisory, investigatory and enforcement activities. Nevertheless, the DPC is committed to providing transparent information to the public around the administration of its office and use of public resources.

Granted	8
Part Granted	3
Refused (OOS)	38
Withdrawn/Handled Outside FOI	8
Live	8
Total requests	65

Ethics in Public Office Act 1995 and Standards in Public Office Act 2001

The DPC was established under the Data Protection Act 2018 and operates in accordance with the provisions of that Act. Procedures are in place to ensure that the staff of the DPC, holding designated positions, comply with the provisions of the Ethics in Public Office Act 1995 and the Standards in Public Office Act 2001.

Regulation of Lobbying Act 2015

The Regulation Lobbying Act 2015 aims to ensure that lobbying activities are conducted in accordance with public expectations of transparency. The Commissioner for Data Protection is a Designated Public Official (DPO) under this Act, as noted on the DPC website. Interactions between lobbying bodies and DPOs must be reported by the lobbyists. The Standards in Public Office Commission (SIPO) has established an online register of lobbying at www.lobbying.ie to facilitate this requirement.

Section 42 of the Irish Human Rights and Equality Commission Act 2014 — Public Sector Equality and Human Rights Duty (the Duty)

The DPC has put in place measures to ensure that consideration is given to human rights and equality in the development of policies, procedures and engagement with stakeholders when fulfilling its mandate to protect the EU fundamental right to data protection. The Duty is also embedded into the Corporate Governance Framework and Customer Charter and Action plan. The DPC website content along with other published information is designed with regard to the principles of plain English, and the DPC has also published audio resources.

To support its customers requiring assistance when engaging with the services provided by the DPC, the DPC's Accessibility Officer may be contacted via the channels listed on its website.

Customer Charter

In 2020, the DPC revised its Customer Charter. The revised Charter and Quality Customer Service Action Plan and Unreasonable Complainants Policy will be in place for the period 2021–2023.

In 2020, 37 customer service complaints were received and resolved by the DPC.



Appendices

Appendix 1: Report on Protected Disclosures received by the Data Protection Commission in 2020

The policy operated by the Data Protection Commission (DPC) under the terms of the Protected Disclosures Act 2014 is designed to facilitate and encourage all workers to raise internally genuine concerns about possible wrongdoing in the workplace so that these concerns can be investigated following the principles of natural justice and addressed in a manner appropriate to the circumstances of the case.

Section 22 of the Protected Disclosures Act 2014 requires public bodies to prepare and publish, by 30 June in each year, a report in relation to the previous year in an anonymised form.

Pursuant to this requirement, the DPC confirms that in 2020

- No internal protected disclosures (from staff of the DPC) were received.

- Nine protected disclosures (set out in the table below) were received from individuals external to the DPC in relation to issues pertaining to data protection within other entities. These cases were raised with the DPC in its role as a 'prescribed person' as provided for under Section 7 of the Protected Disclosures Act (listed in SI 339/2014 as amended by SI 448/2015, replaced in September 2020 by SI 364/2020).

Reference Number	Type	Date Received	Status	Outcome
09/2020	Section 7 (external, to 'prescribed person')	09 December 2020	Under Consideration	
08/2020	Section 7 (external, to 'prescribed person')	16 September 2020	Under Consideration	
07/2020	Section 7 (external, to 'prescribed person')	09 July 2020	Under Consideration	
06/2020	Section 7 (external, to 'prescribed person')	26 May 2020	Closed	Made anonymously and not a protected disclosure — referred to consultation function to follow up.
05/2020	Section 7 (external, to 'prescribed person')	12 May 2020	Closed	Not a protected disclosure – referred to standard complaint handling.
04/2020	Section 7 (external, to 'prescribed person')	28 April 2020	Closed	Not a protected disclosure — referred to standard complaint handling
03/2020	Section 7 (external, to 'prescribed person')	22 February 2020	Closed	Not a protected disclosure- referred to standard complaint handling
02/2020	Section 7 (external, to 'prescribed person')	03 February 2020	Closed	Complainant did not pursue matters.
01/2020	Section 7 (external, to 'prescribed person')	06 January 2020	Closed	Complainant did not pursue matters.

Appendix 2:

Report on Energy Usage at the DPC

Overview of Energy Usage

DUBLIN

21 Fitzwilliam Square

The head office of the DPC is located at 21 Fitzwilliam Square, Dublin 2. Energy consumption for the office is solely electricity, which is used for heating, lighting and equipment usage.

21 Fitzwilliam Square is a protected building and is therefore exempt from the energy rating system.

Satellite office

DPC currently maintains additional office space in Dublin to accommodate the increase in staff numbers. This office was sourced by OPW and DPC took occupancy in October 2018. The Office is 828 sq mts in size.

Energy consumption for the building is solely electricity, which is used for heating, lighting and equipment usage.

The energy rating for the building is C2.

PORTARLINGTON

The Portarlinton office of the DPC has an area of 444 sq mts and is located on the upper floor of a two-storey building, built in 2006.

Energy consumption for the office is electricity for lighting and equipment usage and natural gas for heating.

The energy rating for the building is C1.

Actions undertaken

The DPC participates in the SEAI online system for the purpose of reporting its energy usage in compliance with the European Communities (Energy End-use Efficiency and Energy Services) Regulations 2009 (S.I. No 542 of 2009)

The energy usage for the office for 2019 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Sq.	93,878KwH	
Satellite Office	89,279KwH	
Portarlinton	40,651KwH	49,379

Overview of Environmental policy / statement for the organisation

The DPC is committed to operate in line with Government of Ireland environmental and sustainability policies.

Outline of environmental sustainability initiatives

- Purchase of single use plastics ceased since January 2019
- Replacement of fluorescent lighting with LED lighting in Portarlinton office as units fail or require replacement bulbs
- Sensor lighting in use in one office (Satellite)
- Review of heating system in one office underway (Fitzwilliam Square)
- New tender competition completed for bin collection services to include compost bin service for Portarlinton & Fitzwilliam Square.

Reduction of Waste Generated

- DPC use a default printer setting to print documents double-sided.
- DPC has also introduced dual monitors for staff to reduce the need to print documents to review / compare against other documentation during case work.
- DPC provide general waste and recycling bins at stations throughout the offices.

Maximisation of Recycling

DPC policy is to securely shred all waste paper. Consoles are provided at multiple locations throughout the offices. Shredded paper is recycled.

Sustainable Procurement

DPC procurements and processes are fully compliant with Sustainable Procurement.

Catering contracts stipulate the exclusion of single use plastics.

Appendix 3: Prosecutions in relation to electronic direct marketing complaints

The DPC prosecuted six companies during 2020 for sending unsolicited text messages or electronic mail to customers or former customers or prospective customers without their consent and in one case without a valid address to which the recipient might send a request for such communications to cease. The companies in question were Three Ireland Services (Hutchison) Limited, Mizzoni's Pizza & Pasta Company Limited, AA Ireland Limited, Ryanair DAC, Three Ireland (Hutchison) Limited and Windsor Motors Unlimited Company.

Prosecution of Three Ireland Services (Hutchison) Limited

In June and August 2019, the DPC received two complaints from individuals concerning unsolicited marketing text messages they had received from the telecommunications company Three Ireland Services (Hutchison) Limited. In response to the DPC's investigation of the first complaint, Three explained that although the customer had requested to opt-out of electronic direct marketing, due to a technical error his preference had not been updated on the company's systems. In respect of the second complaint, Three indicated that the actioning of the customer's request to opt-out had been delayed due to a fault which had developed in its case management system as a result of internal IT changes.

The DPC had issued a letter of formal warning to Three in January 2016 in relation to a previous complaint. Accordingly, the DPC decided to proceed to a prosecution arising from these two complaint cases.

At Dublin Metropolitan District Court on 2 March 2020, Three pleaded guilty to two charges under Regulation 13(1) and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €200 to Little Flower Penny Dinners in respect of each of the two charges. Three agreed to discharge the DPC's legal costs.

Prosecution of Mizzoni's Pizza & Pasta Company Limited

In March and April 2019, the DPC received four complaints from individuals regarding unsolicited marketing text messages they had received from Mizzoni's Pizza & Pasta Company Limited. In particular, the complaints highlighted the concern that customers' phone numbers may have been retained for a significant

period after the date of their last order. Following an investigation of the complaints, the DPC was satisfied that Mizzoni's had failed to comply with the rules on valid consent for electronic direct marketing under the ePrivacy Regulations.

The DPC had issued a letter of formal warning to Mizzoni's in November 2013 in respect of a previous complaint. Accordingly, the DPC decided to initiate prosecution action on foot of these new complaints.

At Dublin Metropolitan District Court on 2 March 2020, Mizzoni's pleaded guilty to one offence under Regulation 13(1) and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €200 to Little Flower Penny Dinners. Mizzoni's agreed to discharge the DPC's legal costs.

Prosecution of Three Ireland (Hutchison) Limited

In March, April and June 2020, the DPC received three complaints from individuals concerning unsolicited marketing text messages they had received from the telecommunications company Three Ireland (Hutchison) Limited. In response to the DPC's investigation of the first complaint, Three explained that although the customer had requested to opt-out of electronic direct marketing, due to an intermittent bug in their system, messages such as opt-outs were received but did not trigger the required action. As a result his preference was not updated on the company's system. In respect of the second complaint, Three indicated that the customer's requests to opt-out had not 'fed back' to the system due to a configuration issue arising from internal IT changes. In regards to the third complaint, Three stated that the customer opted out of electronic direct marketing and received confirmation of same. However, due to a human error where

an incorrect set of permissions was used, she received further electronic direct marketing.

The DPC had previously prosecuted Three in 2012 for breaching Regulation 13 of the ePrivacy Regulations in relation to three previous complaints. Accordingly, the DPC decided to proceed to another prosecution arising from these three complaint cases.

At Dublin Metropolitan District Court on 17 December 2020, Three pleaded guilty to four charges under Regulation 13(1) and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €2,000 to Little Flower Penny Dinners. Three agreed to discharge the DPC's legal costs.

Prosecution of AA Ireland Limited

In July and October 2019, the DPC received three complaints from individuals concerning unsolicited marketing text messages and electronic mail they had received from AA Ireland Limited. In response to the DPC's investigation of the first complaint, AA explained that the customer had opted-out of electronic direct marketing in 2017 and this opt-out was applied at that time. However, due to a 'system issue' a couple of years later it was recorded that he had opted-in and he received further electronic direct marketing by email. In respect of the second complaint, AA indicated that it had received the customer's requests to opt-out but due to the customer having completed five different quotes and the opt-out had to be applied to each, this resulted in a delay and the sending of nineteen further marketing text messages over an eight-day period after she had first opted out. In regards to the third complaint, AA stated that the customer had never opted in to receiving electronic direct marketing. It also claimed that the text messages sent were reminders to the customer that their insurance renewal date was approaching and it deemed them transactional messages rather than marketing messages. However, due to the content of the text messages, the DPC deemed them to be unsolicited marketing text messages.

The DPC had previously prosecuted AA in 2018 for breaching Regulation 13 of the ePrivacy Regulations in relation to one previous complaint. Accordingly, the DPC decided to proceed to another prosecution arising from these three complaint cases.

At Dublin Metropolitan District Court on 17 December 2020, AA pleaded guilty to three charges under Regulation 13(1), and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €2,500 to Little Flower Penny Dinners. AA agreed to discharge the DPC's legal costs.

Prosecution of Ryanair DAC

In May 2019, the DPC received a complaint from an individual concerning a marketing email they had received from Ryanair DAC that they were unable to unsubscribe

from. The complainant indicated that having used the unsubscribe button on the email they received from Ryanair they received an error message. They continued to receive further marketing emails subsequently. In response to the DPC's investigation of the complaint, Ryanair explained that due to a technical issue within Adobe Campaign (which Ryanair uses to run its email campaigns) that affected unsubscribe / opt-out requests, customers received the 'error message' referred to in the complaint.

The DPC had issued a letter of formal warning to Ryanair in April 2013 in respect of two previous complaints. Accordingly, the DPC decided to initiate prosecution action on foot of this new complaint.

At Dublin Metropolitan District Court on 17 December 2020, Ryanair pleaded guilty to two charges under Regulation 13(1), 13(12)(c) and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €5,000 to Little Flower Penny Dinners. Ryanair agreed to discharge the DPC's legal costs.

Prosecution of Windsor Motors Unlimited Company

In September 2019, the DPC received three complaints from individuals regarding unsolicited marketing text messages they had received from Windsor Motors Unlimited Company. In response to the DPC's investigation of the first and second complaint, Windsor Motors explained that the former customers had provided their contact details to the company in 2008 when service work was carried out on their vehicles. It admitted that the first time that the mobile phone numbers of those former customers were targeted with marketing messages was in September 2019 – 11 years later. It accepted the DPC's view that it had not kept any marketing consent that it may have obtained in 2008 up-to-date in accordance with the twelve-month rule set out in Regulation 13(11) (d) of the ePrivacy Regulations. In respect of the third complaint, Windsor Motors indicated that it had received the former prospective customer's request to opt-out in 2017 and this opted-out request was actioned. However, almost a year later due to an error when introducing a new IT system the individual's details were inadvertently opted back in to marketing.

The DPC had issued a letter of formal warning to Windsor Motors in July 2017 in respect of a previous complaint received from the prospective customer referred to above. Accordingly, the DPC decided to initiate prosecution action on foot of these new complaints.

At Dublin Metropolitan District Court on 17 December 2020, Windsor Motors pleaded guilty to one offence under Regulation 13(1) and 13(13)(a)(i) of the ePrivacy Regulations. The District Court applied the Probation of Offenders Act 1907, ordering a dismissal of the matter on the basis of a charitable donation of €1,000 to Little Flower Penny Dinners. Windsor Motors agreed to discharge the DPC's legal costs.

Appendix 4:

Twitter International Company — Inquiry (IN-19-1-1) under Section 110 of the Data Protection Act 2018

Twitter International Company – Inquiry (IN-19-1-1) under Section 110 of the Data Protection Act 2018

This inquiry, which was commenced by the DPC on 22 January 2019, examined whether Twitter International Company ('TIC') had complied with its obligations under the GDPR in respect of its notification, on 8 January 2019, of a personal data breach ('the Breach') to the DPC. The Breach, which occurred at TIC's processor, Twitter Inc., related to a bug whereby if a Twitter user with a protected account, using Twitter for Android, changed their email address, their account would become unprotected.

The purpose of the inquiry was to examine certain issues surrounding TIC's notification of the Breach, as distinct from examining the substantive issues relating to the Breach itself. In this regard, the inquiry examined whether TIC had complied with Article 33(1) of the GDPR, in terms of the timing of its notification of the Breach to the DPC, and whether it had complied with Article 33(5) of the GDPR, in respect of its documenting of the Breach.

Facts leading to Inquiry

TIC's notification of the Breach to the DPC, which led to the inquiry, took place on 8 January 2019 by way of a completed Cross-Border Breach Notification Form. In the Form, TIC outlined that it had received a bug report through its 'Bug Bounty Program' to the effect that "... if a Twitter user with a protected account, using Twitter for Android, changed their email address the bug would result in their account being unprotected." The Breach Notification Form further outlined, in respect of the reasons for not notifying the DPC within the 72 hour period required by Article 33(1), that

"The severity of the issue — and that it was reportable — was not appreciated until 3 January 2018 [sic] at which point Twitter's incident response process was put into action."

The Breach Notification Form identified the potential impact for affected individuals, as assessed by TIC, as being "significant". In a further follow up notification form submitted by TIC to the DPC on 16 January 2019, TIC confirmed the number of affected EU and EEA users was 88,726. It also confirmed that the bug which had led to the Breach "was introduced on 4 November 2014 and fully

remediated by 14 January 2019" and that, as it was not possible to identify all impacted persons (due to retention limitations on available logs), it believed that additional people were impacted during that period.

Inquiry under Section 110, Data Protection Act 2018

As it appeared from the Breach Notification Form submitted by TIC that a period of in excess of 72 hours had elapsed from when TIC (as controller) became aware of the Breach, and having regard to the number of affected data subjects, the DPC commenced the inquiry, under Section 110(1) of the Data Protection Act 2018 ('the 2018 Act') for the purpose of examining whether TIC had complied with its obligations under Article 33, and more particularly, with its obligations under Article 33(1) and Article 33(5).

Compliance with Article 33(1)

In assessing TIC's compliance with Article 33(1), the DPC examined the timeline relating to TIC's notification of the Breach to the DPC. In this regard, TIC confirmed to the DPC during the inquiry that notice of the bug was first received on 26 December 2018 by an external contractor engaged by Twitter to search for and assess bugs via the Bug Bounty Program, a program whereby anyone may submit a bug report. TIC further confirmed that, on 29 December 2018, the external contractor, having assessed the bug report, communicated the outcome of its assessment to Twitter Inc. TIC further confirmed that Twitter Inc. then commenced its internal Information Security review of the issue on 2 January 2019, and that, following this, on 3 January 2019, Twitter Inc. assessed the incident as being a potential personal data breach under the GDPR and determined that the incident response plan should be initiated. TIC also confirmed that, following this (on 4 January 2019), an Incident Management (IM) ticket was opened but that, due to a failure (by Twitter Inc. staff) to follow a particular step in the incident management process as it was prescribed, the Data Protection Officer (DPO) for TIC was not added to the IM ticket, which resulted in a delay in the DPO (and, therefore TIC as controller) being notified of the issue.

TIC confirmed to the DPC that it was first made aware of the Breach by its processor, Twitter Inc., on 7 January 2019. It submitted that, in circumstances where it had notified the Breach to the DPC on 8 January 2019, it had complied with the requirement to notify under Article 33(1).

Having considered the timeline in relation to TIC's notification of the Breach, the DPC formed the view that, notwithstanding TIC's actual awareness of the Breach on 7 January 2019, TIC ought to have been aware of the Breach at an earlier point in time and, in this particular case, at the latest by 3 January 2019. In forming this view, the DPC took account of the fact that 3 January 2019 was the date on which Twitter Inc. first assessed the incident as being a potential personal data breach but that, for reasons of the ineffectiveness of the process in the particular circumstances that transpired and/or a failure by Twitter Inc. staff to follow its own incident management process, a delay occurred in the DPO being informed of the potential data breach, which, in turn, resulted in TIC (as controller) not being notified of the Breach until 7 January 2019.

In making this finding, the DPC also took account of an earlier delay that had arisen in the period from when the incident was first notified to Twitter Inc. by its external contractor on 29 December 2018 to when Twitter Inc. commenced its Information Security review of the issue on 2 January 2019. During the course of the inquiry, TIC confirmed to the DPC that this delay had arisen "*due to the winter holiday schedule*" (in circumstances where three of the four days in question were holidays – a weekend and New Years Day) which had led to the issue not being identified and escalated as it should have been. However, the DPC did not accept this delay as being reasonable, in particular in circumstances where potential risks to the data protection and privacy rights of data subjects cannot be neglected, even for a limited period of days, simply because it is an official holiday day/period or a weekend and given that Twitter's services do not cease to operate during such times.

As outlined in the Decision, the alternative application of Article 33(1), and that which was suggested by TIC during the inquiry, whereby the performance by a controller of its obligation to notify is, essentially, contingent upon the compliance by its processor with its obligations under Article 33(2), would undermine the effectiveness of the Article 33 obligations on a controller. Such an approach would be at odds with the overall purpose of the GDPR and the intention of the EU legislator.

Compliance with Article 33(5)

In assessing TIC's compliance with Article 33(5), the DPC carried out a review of the documentation provided by TIC during the course of the inquiry, and in which it claimed that it had documented the Breach.

In doing so, the DPC found that TIC had not complied with Article 33(5). This was in circumstances where the documentation maintained by TIC – either individually or collectively – did not comprise a record, or document,

of, specifically, a 'personal data breach' within the terms of Article 33(5), but rather was documentation of a more generalised nature, including reports and internal communications, that were generated in the course of TIC's management of the incident.

In addition, the DPC found that the documentation maintained by TIC in relation to the Breach did not contain sufficient information so as to enable the question of TIC's compliance with the requirements of Article 33 to be verified, as is required by Article 33(5). In particular, the DPC found that the documentation, which TIC had identified as being the primary record in which it had documented the facts, effects and remedial action taken in respect of the Breach, was deficient in circumstances where it did not contain all material facts relating to the notification of the Breach to the DPC. In particular, the documentation did not contain any reference to the issues that had led to the delay in TIC being notified of the Breach by its processor, nor did it address how TIC had assessed the risk to affected users arising from the Breach. The DPC also found that the deficiencies in the documentation furnished by TIC as a record of the Breach were further demonstrated by the fact that, during the inquiry, the DPC had to raise multiple queries in order to gain clarity concerning the facts surrounding the notification of the Breach.

Process under Article 60 and Article 65 GDPR

On 22 May 2020, the DPC issued a draft of its Decision ('the Draft Decision') to the other concerned supervisory authorities ('CSAs') for their opinion in accordance with the process under Article 60 GDPR. The Draft Decision set out the DPC's proposed finding of infringements under Articles 33(1) and 33(5) and its proposal to impose an administrative fine. Under Article 60(4), CSAs have a period of four weeks within which to express a relevant and reasoned objection to a draft decision.

A number of CSAs expressed objections in relation to aspects of the Draft Decision, including objections on the basis that the DPC should, as part of its inquiry, have considered other provisions of the GDPR; objections relating to non-substantive matters, such as the designation of the role of the respondent under investigation (TIC) and the competence of the DPC, as Lead Supervisory Authority, to deal with the matter; and objections in relation to the administrative fine which the DPC proposed.

Having considered the objections raised, and having endeavoured to reach consensus with the CSAs, the DPC was unable to follow the objections in an amended Draft Decision. On this basis, the DPC referred the matter to the European Data Protection Board (EDPB) for determination pursuant to the Article 65 dispute resolution mechanism. The EDPB commenced the Article 65 procedure on 8 September 2020. Having adopted its binding decision under Article 65(1)(a) ('the EDPB Decision') on 9 November 2020, the EDPB notified same to the DPC on 17 November 2020. Thereafter, pursuant to Article 65(6), the DPC was required to adopt its final

decision on the basis of the EDPB Decision “*without undue delay and at the latest by one month after the Board has notified its decision.*”

Article 65(1)(a) provides that the EDPB’s binding decision under Article 65 “...shall concern all the matters which are the subject of the relevant and reasoned objection, in particular whether there is an infringement of [the GDPR]”. In this regard, in terms of the EDPB’s assessment of the objections raised by the CSAs in this case, the EDPB Decision found that certain of the objections raised were not ‘relevant and reasoned’ within the meaning of Article 4(24) on the basis that they did not provide a clear demonstration as to the significance of the risks posed by the Draft Decision as regards the fundamental rights and freedoms of data subjects and, where applicable, the free flow of personal data within the European Union (as is required by Article 4(24)).

With regard to a number of other objections raised, and which had been made on the basis that the DPC should have considered further infringements under other provisions of the GDPR (specifically, Articles 5(1)(f), 5(2), 24 and 32), whilst the EDPB found that these objections were relevant and reasoned under Article 4(24), it determined that it could not, on the basis of the factual elements in the Draft Decision or in the objections themselves, establish the existence of such further (or alternative) infringements.

Finally, and with regard to the objections raised by CSAs in respect of the administrative fine imposed, the EDPB found that certain of these objections were relevant and reasoned under Article 4(24). As such, the EDPB issued a binding direction to the DPC to re-assess the elements that it had relied upon to calculate the amount of the fine (under Article 83(2) GDPR) and to amend its Draft Decision by increasing the level of the fine. *(For further detail on the EDPB Decision, please refer to the EDPB website where the EDPB Decision is published).*

Decision under Section 111 of 2018 Act

The DPC adopted its final Decision (‘the Decision’) on the basis of the EDPB Decision, pursuant to Article 60(7) in conjunction with Article 65(6), on 9 December 2020. In finding that TIC had infringed both Article 33(1) and Article 33(5), the DPC imposed an administrative fine of \$500,000 (estimated for this purpose at €450,000) which reflected an increase in the level of the proposed administrative fine set out in the Draft Decision, in accordance with the direction of the EDPB. In determining this fine, the DPC ensured, as it is required to do under Article 83(1) GDPR, that the fine imposed was effective, proportionate and dissuasive. In this regard, in deciding to impose a fine and in determining the amount of same, the DPC considered the full range of factors under Article 83(2) GDPR in the context of the circumstances of this particular case. In doing so, the DPC had particular regard to the nature, gravity and duration of the infringements concerned, taking account of the nature, scope and purpose of the processing and the number of data subjects affected. The DPC also had regard to the negligent character of the infringements. In setting the fine, the DPC also took account of certain other factors, including the steps that had been taken by Twitter Inc. to rectify the bug.

In reaching its decision in this case, the DPC also highlighted that controller compliance with the obligations under Article 33(1) and Article 33(5) is of central importance to the overall functioning of the supervision and enforcement regime performed by data protection authorities.

Confirmation by Circuit Court of decision to impose administrative fine

Under Section 143 of the Data Protection Act 2018 (2018 Act), the DPC is required to make an application to the Circuit Court for confirmation of its decision to impose an administrative fine. Such application can only be made when the timeframe (of 28 days), as prescribed by Section 142(1) of the 2018 Act, for an appeal of the decision by the controller or processor concerned has expired. At the time of publication, the timeframe for appeal having expired, the DPC is preparing to make an application to the Circuit Court, under Section 143 of the 2018 Act, for confirmation of its decision in respect of the administrative fine.

Appendix 5:

Litigation concerning Standard Contractual Clauses

Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems **[Record No. 2016/ 4809 P]**

On 31 May 2016, the DPC (then the Data Protection Commissioner) commenced proceedings in the Irish High Court seeking a reference to the Court of Justice of the European Union (CJEU) in relation to the validity of “standard contractual clauses” (SCCs). SCCs are a mechanism, established by a number of EU Commission decisions, under which, at present, personal data can be transferred from the EU to the US. The DPC took these proceedings in accordance with the procedure set out by the CJEU in its 6 October 2015 judgment (which also struck down the Safe Harbour EU to US personal data transfer regime). The CJEU ruled that this procedure (involving seeking a reference to the CJEU) must be followed by an EU data protection authority (DPA) where a complaint which is made by a data subject concerning an EU instrument, such as an EU Commission decision, is considered by the EU DPA to be well founded.

(1) Background

The proceedings taken by the DPC have their roots in the original complaint made in June 2013 to the DPC about Facebook by Mr Maximilian Schrems concerning the transfer of personal data by Facebook Ireland to its parent company, Facebook Inc., in the US. Mr Schrems was concerned that, because his personal data was being transferred from Facebook Ireland to Facebook Inc., his personal data was then being accessed (or was at risk of being accessed) unlawfully by US state security agencies. Mr Schrems’ concerns arose in light of the disclosures by Edward Snowden regarding certain programmes said to be operated by the US National Security Agency, most notably a programme called “PRISM”. The DPC had declined to investigate that complaint on the grounds that it concerned an EU Commission decision (which established the Safe Harbour regime for transferring data from the EU to the US) and on that basis he was bound under existing national and EU law to apply that EU Commission decision. Mr Schrems brought a judicial review action against the decision not to investigate his complaint and that action resulted in the Irish High Court making a reference to the CJEU, which in turn delivered its decision on 6 October 2015.

(2) CJEU procedure on complaints concerning EU Commission decisions

The CJEU ruling of 6 October 2015 made it clear that where a complaint is made to an EU DPA which involves a claim that an EU Commission decision is incompatible with protection of privacy and fundamental rights and freedoms, the relevant DPA must examine that complaint even though the DPA cannot itself set aside or disapply that decision. The CJEU ruled that if the DPA considers the complaint to be well founded, then it must engage in legal proceedings before the national Court and, if the national Court shares those doubts as to the validity of the EU Commission decision, the national Court must then make a reference to the CJEU for a preliminary ruling on the validity of the EU Commission decision in question. As noted above, the CJEU in its judgment of 6 October 2015 also struck down the EU Commission decision which underpinned the Safe Harbour EU to US data transfer regime.

(3) DPC’s draft decision

Following the striking down of the Safe Harbour personal data transfer regime, Mr Schrems reformulated and resubmitted his complaint to take account of this event and the DPC agreed to proceed on the basis of that reformulated complaint. The DPC then examined Mr Schrems’ complaint in light of certain articles of the EU Charter of Fundamental Rights (the Charter), including Article 47 (the right to an effective remedy where rights and freedoms guaranteed by EU law are violated). In the course of investigating Mr Schrems’ reformulated complaint, the DPC established that Facebook Ireland continued to transfer personal data to Facebook Inc. in the US in reliance in large part on the use of SCCs. Arising from her investigation of Mr Schrems’ reformulated complaint the DPC formed the preliminary view (as expressed in a draft decision of 24 May 2016 and subject to receipt of further submissions from the parties) that Mr Schrems’ complaint was well founded. This was based on the DPC’s draft finding that a legal remedy compatible with Article 47 of the Charter is not available in the US to EU citizens whose data is transferred to the US where it may be at risk of being accessed and processed by US State agencies for national security purposes in a manner incompatible with Articles 7 and 8 of the Charter. The DPC also formed the preliminary view that SCCs do not address this lack of an effective Article 47-compatible remedy and that SCCs themselves are therefore likely to offend against Article

47 insofar as they purport to legitimise the transfer of the personal data of EU citizens to the US.

(4) The Proceedings and the Hearing

The DPC therefore commenced legal proceedings in the Irish High Court seeking a declaration as to the validity of the EU Commission decisions concerning SCCs and a preliminary reference to the CJEU on this issue. The DPC did not seek any specific relief in the proceedings against either Facebook Ireland or Mr Schrems. However, both were named as parties to the proceedings in order to afford them an opportunity (but not an obligation) to fully participate because the outcome of the proceedings would impact on the DPC's consideration of Mr Schrems' complaint against Facebook Ireland. Both parties chose to participate fully in the proceedings. Ten interested third parties also applied to be joined as *amicus curiae* ("friends of the court") to the proceedings and the Court ruled four of those ten parties (the US Government, BSA The Software Alliance, Digital Europe and EPIC (Electronic Privacy Information Centre)) should be joined as *amici*.

The hearing of the proceedings before Ms Justice Costello in the Irish High Court (Commercial Division) took place over 21 days in February and March 2017 with judgment being reserved at the conclusion of the hearing. In summary, legal submissions were made on behalf of: (i) each of the parties, being the DPC, Facebook Ireland and Mr Schrems; and (ii) each of the "friends of the Court", as noted above. The Court also heard oral evidence from a total of five expert witnesses on US law, as follows:

- Ms Ashley Gorski, expert witness on behalf of Mr Schrems;
- Professor Neil Richards, expert witness on behalf of the DPC;
- Mr Andrew Serwin, expert witness on behalf of the DPC;
- Professor Peter Swire, expert witness on behalf of Facebook; and
- Professor Stephen Vladeck, expert witness on behalf of Facebook.

In the interim period between the conclusion of the trial and the delivery of the judgment on 3 October 2017 (see below), a number of updates on case law and other developments were provided by the parties to the Court.

(5) Judgment of the High Court

Judgment was delivered by Ms Justice Costello on 3 October 2017 by way of a 152 page written judgment. An executive summary of the judgment was also provided by the Court.

In the judgment, Ms Justice Costello decided that the concerns expressed by the DPC in her draft decision of 24 May 2016 were well-founded, and that certain of the issues raised in these proceedings should be referred to the CJEU so that the CJEU could make a ruling as to the validity of the EU Commission decisions which established SCCs as a method of carrying out personal

data transfers. In particular the Court held that the DPC's draft findings as set out in her draft decision of 24 May 2016 that the laws and practices of the US did not respect the right of an EU citizen under Article 47 of the Charter to an effective remedy before an independent tribunal (which, the Court noted, applies to the data of all EU data subjects whose data has been transferred to the US) were well-founded.

In her judgment of 3 October 2017, Ms. Justice Costello also decided that, as the parties had indicated that they would like the opportunity to be heard in relation to the questions to be referred to the CJEU, she would list the matter for submissions from the parties and then determine the questions to be referred to the CJEU. The parties to the case, along with the *amicus curiae* made submissions to the Court, amongst other things, on the questions to be referred, on 1 December 2017 and on 16, 17 and 18 January 2018. During these hearings, submissions were also made on behalf of Facebook and the US Government as to "errors" which they alleged had been made in the judgment of 3 October 2017. The Court reserved its judgment on these matters.

(6) Questions to be referred to the CJEU

On 12 April 2018, Ms. Justice Costello notified the parties of her Request for a Preliminary Ruling from the CJEU pursuant to Article 267 of the TFEU. This document sets out the 11 specific questions to be referred to the CJEU, along with a background to the proceedings.

On the same date, Ms Justice Costello also indicated that she had made some alterations to her judgment of 3 October 2017, specifically to paragraphs 175, 176, 191, 192, 207, 213, 215, 216, 220, 221 and 239. During that hearing, Facebook indicated that it wished to consider whether it would appeal the decision of the High Court to make the reference to the CJEU and if so, seek a stay on the reference made by the High Court to the CJEU. On that basis, the High Court listed the matter for 30 April 2018.

When the proceedings came before the High Court on 30 April 2018, Facebook applied for a stay on the High Court's reference to the CJEU pending an appeal by it against the making of the reference. Submissions were made by the parties in relation to Facebook's application for a stay.

On 2 May 2018, Ms. Justice Costello delivered her judgment on the application by Facebook for a stay on the High Court's reference to the CJEU. In her judgment, Ms Justice Costello refused the application by Facebook for a stay, holding that the least injustice would be caused by the High Court refusing any stay and delivering the reference immediately to the CJEU.

(7) Appeal to the Supreme Court

On 11 May 2018, Facebook lodged an appeal, and applied for leave to appeal to the Supreme Court, against the judgments of 3 October 2017, the revised judgment of 12 April 2018 and the judgment of 2 May 2018 refusing

a stay. Facebook's application for leave to appeal to the Supreme Court was heard on 17 July 2018. In a judgment delivered on 31 July 2018, the Supreme Court granted leave to Facebook allowing it to bring its appeal in the Supreme Court but leaving open the question as to what was the nature of the appeal which was allowed to be brought to the Supreme Court. During late 2018, there were several procedural hearings in the Supreme Court in preparation for the substantive hearing. The substantive hearing of the appeal took place over 21, 22 and 23 January 2018 before a five judge Supreme Court panel composed of the Chief Justice – Mr Justice Clarke, Mr Justice Charleton, Ms Justice Dunne, Ms Justice Finlay Geoghegan and Mr Justice O'Donnell. Oral arguments were made on behalf of Facebook, the DPC, the US Government and Mr Schrems. The central questions arising from the appeal related to whether, as a matter of law, the Supreme Court could revisit the facts found by the High Court relating to US law. This arose from allegations by Facebook and the US Government that the High Court judgment, which underpinned the reference made to the CJEU, contained various factual errors concerning US law.

On 31 May 2019 the Supreme Court delivered its main judgment, which ran to 77 pages. In summary, the Supreme Court dismissed Facebook's appeal in full. In doing so, the Supreme Court decided that:

- It was not open to it as a matter of Irish and EU law to entertain any appeal against a decision of the High Court to make a reference to the CJEU. Neither was it open to the Supreme Court to entertain any appeal in relation to the terms of such a reference (i.e. the specific questions which the High Court had referred to the CJEU). The Supreme Court decided that the issue of whether to make a reference to the CJEU is a matter solely for the Irish High Court. Therefore it was not appropriate for the Supreme Court to consider, in the context of Facebook's appeal, the High Court's analysis which led to the decision that it shared the concerns of the DPC in relation to the validity of the SCC decision. This was because this issue was inextricably linked to the High Court's decision to make a reference to the CJEU and it was not open to Facebook to pursue this as a point of appeal.
- However it was open to the Supreme Court to consider whether the facts found by the High Court (i.e. those facts which underpinned the reference made to the CJEU) were sustainable by reference to the evidence which had been placed before the High Court, or whether those facts should be overturned.
- Insofar as Facebook disputed certain key issues of fact which had been found by the High Court concerning US law, on the basis of the expert evidence before the High Court, the Supreme Court had not identified any findings of fact which were unsustainable. Accordingly, the Supreme Court did not overturn any of the facts found by the High Court. Instead the Supreme Court was of the view that the criticisms which Facebook had made of the High Court judgment concerned the proper characterisation of the underlying facts rather than the actual facts.

(8) Hearing before the CJEU

The CJEU (Grand Chamber) held an oral hearing in respect of the reference made to it by the Irish High Court on 9 July 2019. The CJEU sat with a composition of 15 judges, including the President of the CJEU, Judge Koen Lenaerts. The appointed Judge Rapporteur was Judge Thomas von Danwitz. The Advocate General assigned to the case was Henrik Saugmandsgaard Øe.

At the hearing, the DPC, Mr Schrems and Facebook made oral submissions before the CJEU. The four parties who were joined as *amicus curiae* ("friends of the court") to the case before the Irish Court (the USA, EPIC, BSA Business Software Alliance Inc. and Digital Europe) were also permitted to make oral submissions. In addition, the European Parliament, the EU Commission and a number of Member States (Austria, France, Germany, Ireland, Netherlands, and the UK) who each intervened in the proceedings also made oral submissions at the hearing before the CJEU. Additionally, at the invitation of the CJEU, the European Data Protection Board (EDPB) addressed the CJEU on specific issues.

(9) Opinion of the Advocate General

The Opinion of Advocate General Saugmandsgaard Øe (the AG) was delivered on 19 December 2019.

In this Opinion, as preliminary matters, the AG noted that the DPC had brought proceedings in relation to Mr Schrems' complaint before the national referring Court in accordance with paragraph 65 of the CJEU's judgment of 6 October 2015 (as described further above). The AG also found that the request for a preliminary ruling was admissible.

In relation to the questions referred to the CJEU by the Irish High Court, the AG expressly limited his consideration to the validity of the EU Commission Decision underlying the SCCs (SCCs Decision). At the outset, the AG noted that his analysis in the Opinion was guided by the desire to strike a balance between the need to show a reasonable degree of pragmatism in order to allow interaction with other parts of the world and the need to assert the fundamental values recognised in the legal orders of the EU, its Member States and the Charter of Fundamental Rights. He was also of the view that the SCCs Decision must be examined with reference to the provisions of the GDPR (as opposed to the Data Protection Directive (Directive 95/46)) in line with Article 94(2) GDPR and the AG also noted that the relevant provisions of the GDPR essentially reproduce the corresponding provisions of the Data Protection Directive.

The AG considered that EU law applies to a transfer of personal data from a Member State to a third country where that transfer forms part of a commercial activity. In this regard, the AG's view was that EU law applies to a transfer of this nature regardless of whether the personal data transferred may be processed by public authorities of that third country for the purpose of protecting national security of that country. As regards the nature of the SCCs, the AG opined that the SCCs represent a general mechanism applicable to transfers irrespec-

tive of the third country of destination and the level of protection guaranteed there.

As regards the test for the level of protection which is required in relation to the safeguards (which may be provided by SCCs) contemplated by Article 46 of the GDPR where personal data is being transferred out of the EU to a third country which does not have an adequacy finding, the AG's opinion was that the level of protection as offered by such safeguards must be essentially equivalent to that offered to data subjects in the EU by the GDPR and the Charter of Fundamental Rights. As such, the requirements of protection of fundamental rights guaranteed by the Charter do not vary according to the legal basis for the data transfer.

Following a detailed examination of the nature and content of the SCCs, the AG concluded that the SCCs Decision was not invalid with reference to the Charter. In his view, because the purpose of the SCCs was to compensate for any deficiencies in the protection of personal data offered by the third country, the validity of the SCCs Decision could not be dependent on the level of protection in the third country. Rather the question of validity must be evaluated by reference to the soundness of the safeguards offered by the SCCs to remedy the deficiencies in protection in the third country. This evaluation must also take account of the safeguards consisting of the powers of supervisory authorities under the GDPR. As the SCCs place responsibility on the controller (the exporter), and in the alternative supervisory authorities, this meant that transfers must be assessed on a case by case basis by the controller, and in the alternative by the supervisory authority, to assess whether the laws in the third country were an obstacle to having an adequate level of protection for the transferred data, such that data transfers must be prohibited or suspended.

The AG then went on to consider the nature of the obligations on the controller carrying out the export of the personal data, which included, according to the AG, a mandatory obligation to suspend a data transfer or terminate a contract with the importer if the importer could not comply with the provisions of the SCCs. The AG also considered the obligations on the importer in this regard and made certain observations about the nature of the examination of the laws of the third country which should be carried out by the exporter and the importer.

The AG also referred to the rights of data subjects who believe there has been a breach of the SCC clauses to complain to supervisory authorities, and went on to consider what he considered the role of the supervisory authority was in this context. In essence, the AG considered that where, following an examination, a supervisory authority considers that data transferred to a third country does not benefit from appropriate protection because the SCCs are not complied with, adequate measures should be taken by the authority to remedy this illegality, if necessary by ordering suspension of the transfer. The AG noted the DPC's submissions that the power to suspend transfers could only be exercised on a case by case basis and would not address systemic issues arising from an adequate lack of protection in a third country. On this point, the AG pointed to the

practical difficulties linked to a legislative choice to make supervisory authorities responsible for ensuring data subjects' rights are observed in the context of transfers or data flows to a specific recipient but said that those difficulties did not appear to him to render the SCC Decision invalid.

Although noting that the question as to the validity of the Privacy Shield was not explicitly referred to the CJEU by the Irish High Court, the AG considered that some of the questions raised by the Irish High Court indirectly raised the validity of the finding of adequacy which the EU Commission made in respect of the Privacy Shield. The AG considered that it would be premature for the Court to rule on the validity of the Privacy Shield in the context of this reference although he noted that answers to the questions raised by the Irish High Court in relation to the Privacy Shield could ultimately be helpful to the DPC later in determining whether the transfers in question should actually be suspended because of an alleged absence of appropriate safeguards. However the AG also referred to the possibility that the DPC could in the subsequent examination of Mr Schrems' complaint, following the delivery of the Court's judgment, decide that it could not determine the complaint unless the CJEU first ruled on whether the existence of the Privacy Shield itself was an obstacle to the DPC exercising the power to suspend the transfers in question. The AG noted that in such circumstances, if the DPC had doubts about the validity of the Privacy Shield, it would be open to the DPC to bring the matter before the Irish Court again in order to seek that another reference on this point be made to the CJEU.

However, despite the AG taking the position that the Court should, in the context of this reference, refrain from ruling on the validity of the Privacy Shield in its judgment, he went on to express, in the alternative, some "non-exhaustive observations" on the effects and validity of the Privacy Shield decision. These observations were set out over approximately 40 pages of detailed analysis, including an analysis of the scope of what the "essential equivalence" of protection in a third party state involved, the possible interferences with data subject rights in relation to data transferred to the US as posed by national intelligence agencies, the necessity and proportionality of such interferences and the laws and practices of the US, including those relating to the question of whether there is an effective judicial remedy in the US for persons whose data has been transferred to the US and whose data protection rights have been subject to interferences by the US intelligence agencies. Having carried out this analysis, the AG ultimately concluded by expressing doubts as to the conformity of the Privacy Shield with provisions of EU law.

(10) Judgment of the CJEU

The CJEU delivered its judgment on 16 July 2020.

In summary:

- The judgment addressed a number of points applicable to transfers generally; amongst other things, the court affirmed, as a core principle of EU law, the

proposition that, when an EU citizen's personal data is transferred to a third country, he or she must be afforded a level of protection in respect of their personal data that is essentially equivalent to that guaranteed within the EU; importantly, the Court also clarified that that proposition holds true irrespective of the legal mechanism deployed to justify a given transfer.

- The CJEU upheld the validity of Commission Decision 2010/87/EU, being a decision by which the EU Commission adopted the SCCs. It follows that the SCCs remain available for use by controllers and processors in connection with transfers to third countries, subject to compliance with certain key points of principle articulated by the Court in the course of its judgment.
- In that regard, the CJEU clarified the nature and extent of the obligations to which data exporters — and national DPAs — are subject in any case where SCCs are relied on to justify data transfers to a third country.
- In particular, the Court outlined the steps to be taken by controllers, prior to engaging in data transfers under the SCCs, to verify, on a case-by-case basis and, where appropriate, in collaboration with the data importer, whether the law of the third country to which the data is to be transferred ensures adequate protection under EU law.
- Equally, the Court confirmed that, if, upon investigation, a national DPA concludes that a data subject whose personal data have been transferred to a third country is not in fact afforded an adequate level of protection in that country, the national supervisory authority must, as a matter of EU law, take appropriate action to remedy any findings of inadequacy and, to that end, exercise one or more of the corrective measures identified in 58(2) of the GDPR.
- A good deal of the Court's analysis was directed to an assessment of the protections afforded to EU citizens in the context of EU-US data transfers. In that regard, the Court found that, while the domestic law of the US imposes certain limitations on US public authorities' right of access to, and use of, transferred data in particular contexts, those limitations do not provide a level of protection essentially equivalent to that required by EU law.
- Against that backdrop, the Court held that the decision by which the EU Commission adopted the "Privacy Shield" arrangements for EU-US data transfers, was invalid. More generally, the judgment may also be read as sounding, at the very least, a strong note of caution in relation to the use of SCCs for data transfers to the US,

GDPR. On that score, the Court was emphatic in terms of the confirmation given (at paragraph 89 of the judgment) that the GDPR "*applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.*"

The level of protection required

At paragraph 95 of the judgment, the Court noted that Recital 107 of the GDPR states that, where "*a third country, a territory or a specified sector within a third country ... no longer ensures an adequate level of data protection. ... the transfer of personal data to that third country ... should be prohibited unless the requirements [of the GDPR] relating to transfers subject to appropriate safeguards ... are fulfilled*".

As regards the level of protection required by the GDPR in the context of transfers to third countries, the Court found, at paragraph 91 of the judgment, and by reference to Articles 46(1) and 46(2)(c) of the GDPR, that, in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country if, and only if:

- (i) the controller or processor has provided 'appropriate safeguards' (which may include the SCCs); and,
- (ii) on condition that *enforceable data subject rights and effective legal remedies* are available to data subjects.

Noting that Article 46 does not identify, with specificity, what is meant by the terms "appropriate safeguards", "enforceable rights" and "effective legal remedies", the Court held that, in circumstances where Article 44 provides that 'all provisions [in that chapter] shall be applied in order to ensure that the level of protection of natural persons guaranteed by [that regulation] is not undermined', it follows that the same level of protection must be maintained when personal data is transferred to a third country, irrespective of the legal mechanism under which that transfer takes place (paragraph 92 of the judgment).

Referencing Recital 108, the Court also noted (at paragraph 95 of the judgment), that, in the absence of an adequacy decision, the 'appropriate safeguards' to be put in place by the controller or processor in accordance with Article 46(1) must 'compensate for the lack of data protection in [the] third country' in order to "ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union".

Accordingly, using the language it had previously deployed in its judgment in the earlier case of *Schrems v. Data Protection Commissioner*, (Case C-362/14, EU:C:2015:650, 6 October 2015), the Court noted, at paragraph 96, that, in circumstances where Chapter V of the GDPR is intended to ensure that the same high level of protection afforded to data subjects within the EU is maintained if and when their data is transferred to a

Points applicable to transfers generally

Public authority access to transferred data for public security, defence and State security purposes

The first substantive issue addressed by the Court saw it rejecting the suggestion that public authority access to transferred data for the purposes of public security, defence and State security falls outside the scope of the

third country, it follows that, in any case where personal data is being transferred to a third country, the level of protection required is one that is “essentially equivalent” to that which is guaranteed within the European Union”.

The Court’s treatment of the SCCs

Application of the SCCs in practice

At paragraph 126 of its judgment, the Court observed that, while the protections built into the SCCs may facilitate the achievement of a level of protection that meets the “essential equivalence” test in the case of transfers to some third countries, the laws and practices of other third countries may be such as to render the SCCs incapable of achieving that level of protection. The Court expressed this point in the following terms:

“Therefore, although there are situations in which, depending on the law and practices in force in the third country concerned, the recipient of such a transfer is in a position to guarantee the necessary protection of the data solely on the basis of standard data protection clauses, there are others in which the content of those standard clauses might not constitute a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. That is the case, in particular, where the law of that third country allows its public authorities to interfere with the rights of the data subjects to which that data relates.”

Having pointed out at paragraph 128 of the judgment that the safeguards to be adduced by the controller are not required to have their origin in a particular decision adopted by the EU Commission, the Court went on to note, at paragraph 132, that, in any case where the SCCs cannot, in and of themselves, achieve the level of protection required as a matter of EU law, the controller may add other clauses or adduce additional safeguards to supplement the SCCs.

Taking this a step further, the Court noted, at paragraph 133, that the SCCs are, in essence, a baseline provision, comprising a set of contractual guarantees intended to apply uniformly in all third countries. If and to the extent the SCCs cannot achieve the level of protection required under EU law in the context of transfers to a particular third country, it follows that transfers to that third country may only proceed if supplementary measures are adopted by the controller.

The practical application of these points of principle was addressed in paragraphs 134, 135, 141 and 142 of the judgment. In summary terms, the Court pointed out that, in circumstances where the SCCs cannot be deployed as a “one size fits all” solution, capable of achieving the required standard of protection in the case of all transfers to all third countries, it necessarily follows that an assessment is required to determine (and verify) whether the laws of the third country of destination in fact ensure adequate protection to the standard required by EU law where personal data is transferred under the SCCs, and, if not, whether additional safeguards can be provided by the controller to compensate for any shortfall.

The Court clarified that, in the first instance, such an assessment must be carried out by the controller or processor, with the input of the data’s intended recipient, where appropriate. Importantly, the assessment referenced by the Court is one that must be carried out on a case-by-case basis, prior to the commencement of transfers by the controller/processor in question to that third country.

Given their centrality to the Court’s analysis, paragraphs 134 and 135 in particular bear setting out in full:

“134. In that regard, as the Advocate General stated in point 126 of his Opinion, the contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the responsibility of the controller or his or her subcontractor established in the European Union and, in the alternative, of the competent supervisory authority. It is therefore, above all, for that controller or processor to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses.

135. Where the controller or a processor established in the European Union is not able to take adequate additional measures to guarantee such protection, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned. That is the case, in particular, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data.”

It will be noted that, at paragraph 135, the Court expressly cautioned that, in the case of some third countries, it may well be the case that no amount of supplemental or additional safeguards will be capable of addressing shortfalls in the level of protection available. In such a scenario, the Court’s position was very clear: such transfers are not permissible; if the controller/processor nonetheless proceeds, it will be a matter for the relevant DPA to intervene to suspend or otherwise end the transfer of personal data to such third country.

The role of data protection supervisory authorities

At paragraphs 111 to 113 of the judgment (and again at paragraph 146), the Court emphasised the central role to be played by national DPAs in connection with the regulation of data transfers to third countries conducted under the SCCs. In that regard, the Court noted that, whilst, in the first instance, it is a matter for the relevant controller/processor to perform the assessment described above, the national DPAs must intervene in any case where (i) the SCCs cannot be complied with in the

third country in question, so that the level of protection required by EU law cannot be ensured; and (ii) the controller or processor has not itself suspended or put an end to the transfer.

The Court put the matter in the following terms:

“111. If a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required, under EU law, to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. To that effect, Article 58(2) of that regulation lists the various corrective powers which the supervisory authority may adopt.

112. Although the supervisory authority must determine which action is appropriate and necessary and take into consideration all the circumstances of the transfer of personal data in question in that determination, the supervisory authority is nevertheless required to execute its responsibility for ensuring that the GDPR is fully enforced with all due diligence.

113. In that regard, as the Advocate General also stated in point 148 of his Opinion, the supervisory authority is required, under Article 58(2)(f) and (j) of that regulation, to suspend or prohibit a transfer of personal data to a third country if, in its view, in the light of all the circumstances of that transfer, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.”

Conclusion re: validity of the SCCs

Having completed its analysis of the SCCs and their application in practice, and having noted that, in principle, they may be utilised (with additional safeguards, where necessary), to achieve the level of protection required by EU law (with appropriate mechanisms available for the suspension of transfers in any case where such protections are compromised), the Court concluded as follows:

“It follows that the SCC Decision provides for effective mechanisms which, in practice, ensure that the transfer to a third country of personal data pursuant to the standard data protection clauses in the annex to that decision is suspended or prohibited where the recipient of the transfer does not comply with those clauses or is unable to comply with them” (paragraph 148).

Accordingly, on the basis of the analysis set out in its judgment, the Court was satisfied to confirm that the SCC Decision was valid.

Privacy Shield and the position in relation to the US

The Court commenced its analysis by recalling that, in principle, public authority access to an individual's personal data with a view to its retention or use constitutes an interference with the fundamental rights enshrined at Articles 7 and 8 of the Charter (see paragraphs 170 and 171 of the judgment).

Whilst noting that such rights are not absolute, the CJEU went on to revisit (at paragraph 174 and subsequent paragraphs) existing principles pursuant to which any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Reference was also made in this context to the following matters:

- the fact that, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others;
- the fact that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned (paragraph 175); and,
- the fact that, in order to satisfy the requirement of proportionality, the legislation making provision for such interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that (in the context of data transfers) the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse (paragraph 176).

From there, the Court went on to identify certain specific failings associated with a number of identified US law measures, including Section 702 FISA, EO 12333 and PPD-28, before concluding (at paragraph 185) that,

“... the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52(1) of the Charter.”

Separately, the Court noted that the EU Commission's finding in the Privacy Shield Decision — that the US ensures a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter — had been called into question on the grounds, inter alia, that the Privacy Shield Ombudsperson cannot remedy the deficiencies which the EU Commission itself had found in connection with the judicial protection of persons whose personal data is transferred to the US. Having analysed relevant elements of the Ombudsperson arrangements by reference to applicable EU law principles, the Court

ultimately concluded (at paragraph 197) that *“the ombudsperson mechanism ... does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.”*

Relatedly, the Court noted (at paragraph 191 of its judgment) that in recital 115 of the Privacy Shield Decision, the EU Commission had itself found that *“while individuals, including EU data subjects, ... have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered”*. The Court considered that the existence of such a “lacuna” in judicial protection in respect of interferences with intelligence programmes based on [PPD-28] *“makes it impossible to conclude, as the Commission did in the Privacy Shield Decision, that United States law ensures a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.”*

The Court also noted (at paragraph 192) that *“neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities from which it follows that data subjects have no right to an effective remedy.”*

Against that backdrop, the Court held (at paragraph 198) that, in reaching its finding in Article 1(1) of the Privacy Shield Decision, that the US ensures an adequate level of protection for personal data transferred from the Union to organisations in that third country under the EU-US Privacy Shield, the EU Commission had *“disregarded the requirements of Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter.”* From there, the Court concluded (at paragraph 199) that *“[i]t follows that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.”*

On the basis that Article 1 of the Privacy Shield Decision was *“inseparable from Articles 2 and 6 of, and the annexes to, that decision”*, the Court took the view that the invalidity of Article 1 *“affects the validity of the decision in its entirety.”* Accordingly, the Court concluded (at paragraph 201) that the Privacy Shield Decision as a whole was invalid.

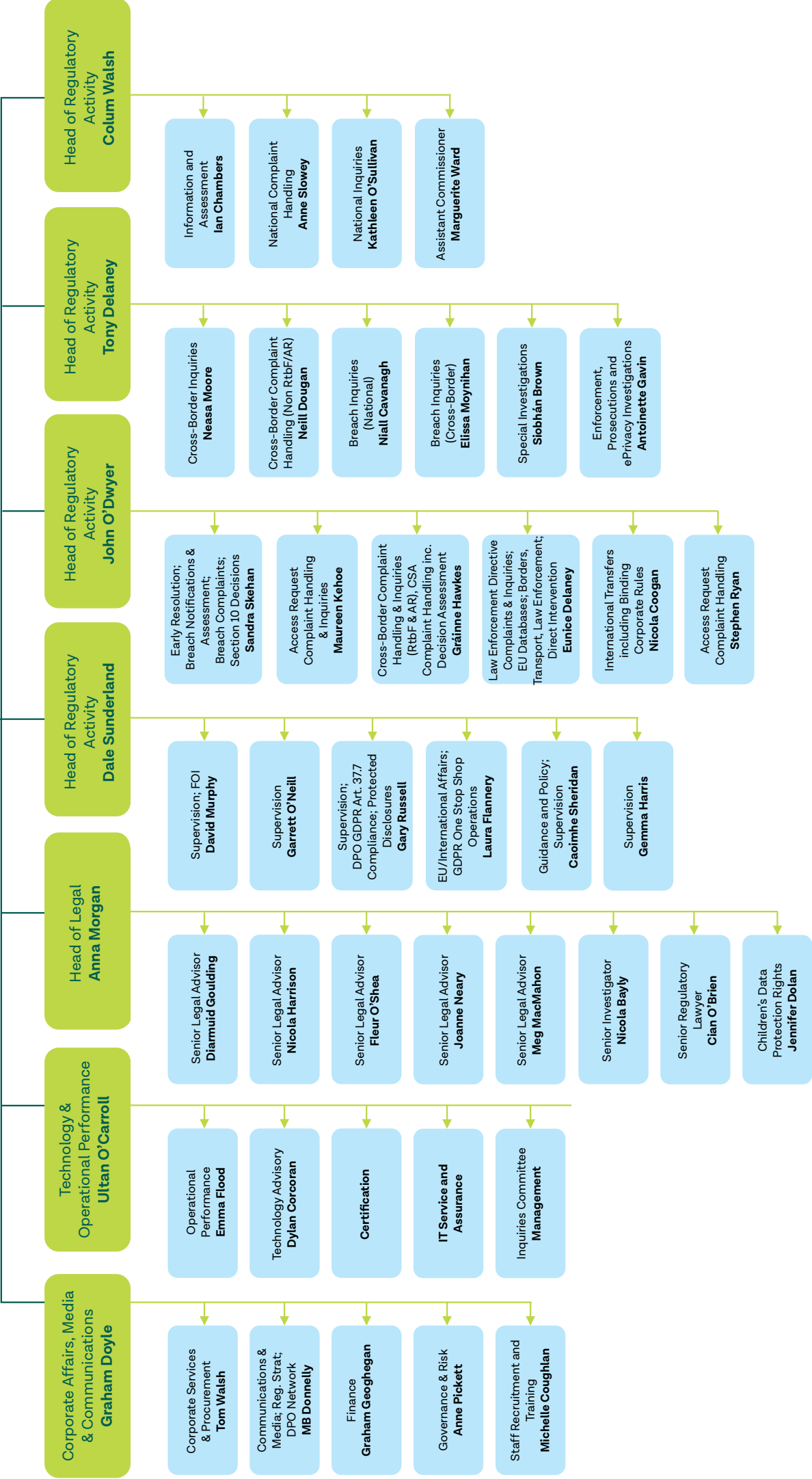


Appendix 6:

Financial Statement for the Year 1 January to 31 December 2020 and the DPC's Statement of Internal Controls

The Financial Statement of the Data Protection Commission for the year 1 January to 31 December 2020 and its Statement of Internal Controls for the same period are in preparation by the DPC and will be appended to this report following completion of an audit in respect of 2020 by the Comptroller and Auditor General.

Commissioner
Helen Dixon



Data Protection Commission,
21 Fitzwilliam Square,
Dublin 2.

www.dataprotection.ie
Email: info@dataprotection.ie



**An Coimisiún um
Chosaint Sonraí**
Data Protection
Commission