

Annual Report
1 January — 31 December 2019



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

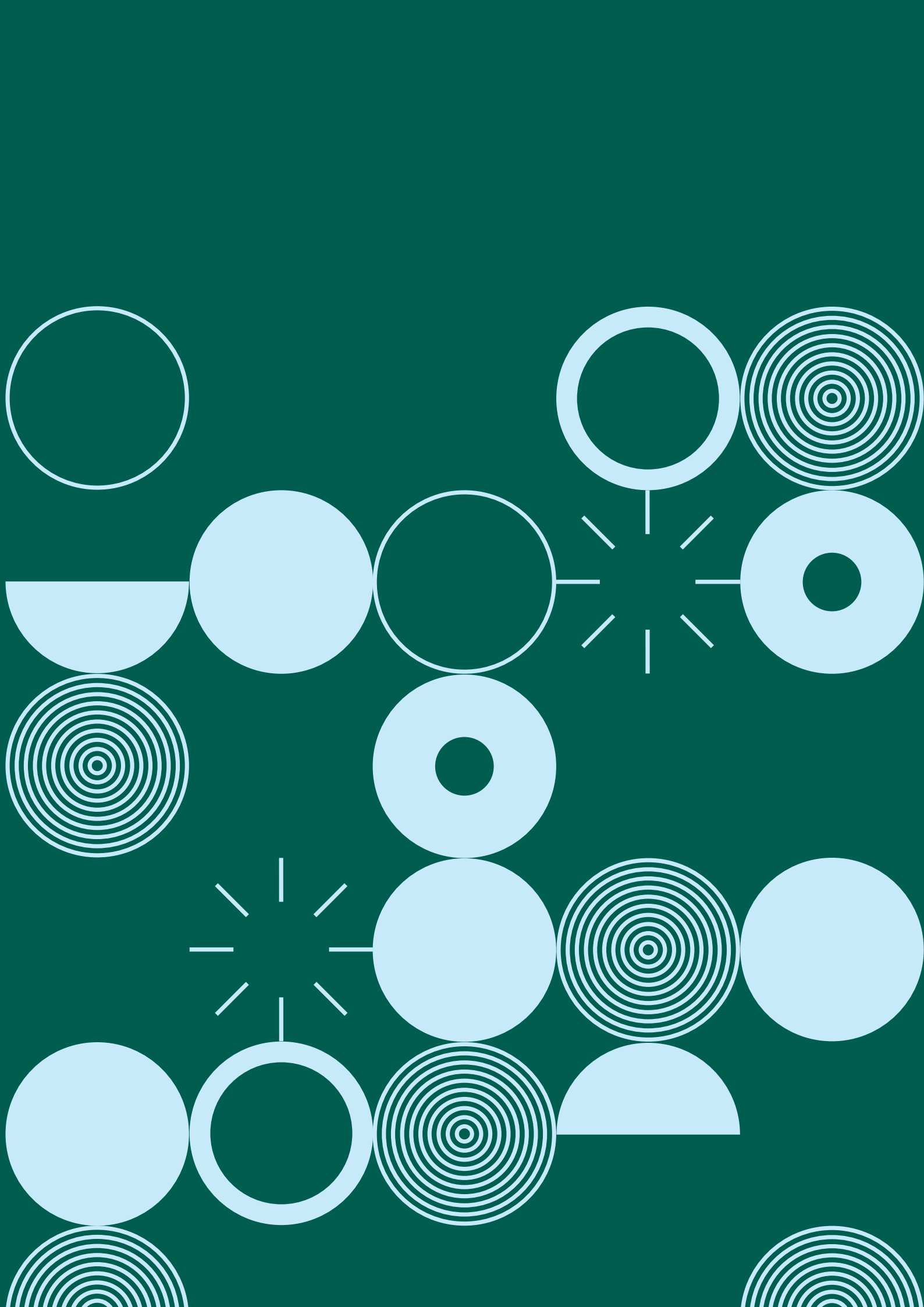


Table of Contents

Foreword	6
Roles and Responsibilities	10
Review of 2019	12
Information and Assessment	16
Complaints	18
Breaches	34
Inquiries	38
Legal Affairs	52
Supervision	56
Data Protection Officers	62
International Activities	64
Processing Children’s Personal Data	68
Communications	70
Key DPC Projects	74
Corporate Affairs	76
 APPENDICES	
Appendix 1: Court of Justice of the European Union (CJEU) Case Law	81
Appendix 2: Litigation concerning Standard Contractual Clauses	89
Appendix 3: Investigation by the DPC into the processing of personal data by DEASP in relation to the Public Services Card	93
Appendix 4: Statement of Internal Controls in Respect of the DPC for the period 1 January 2019 to 31 December 2019	95
Appendix 5: Report on Protected Disclosures received by the Data Protection Commission in 2019	97
Appendix 6: Financial Statements for the Year 1 January to 31 December 2019	98

KNOW YOUR DATA

A DPC PODCAST

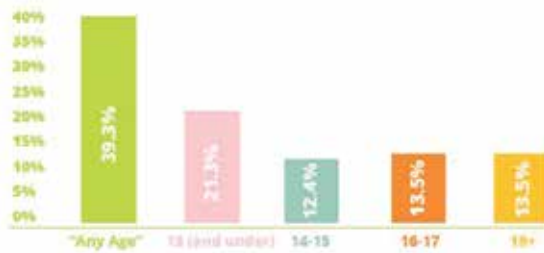
2019



An Commission um
Chosaint Soisial
Data Protection
Commission



Q3. WHAT AGE DO YOU THINK YOU SHOULD HAVE TO BE BEFORE YOU CAN ASK ANY COMPANY FOR A COPY OF YOUR PERSONAL DATA, OR BEFORE YOU CAN TELL THEM TO DELETE YOUR PERSONAL DATA?



An Commission um
Chosaint Soisial
Data Protection
Commission



An Commission um
Chosaint Soisial
Data Protection
Commission

DPO Conference

Save the date: 31 March 2020



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

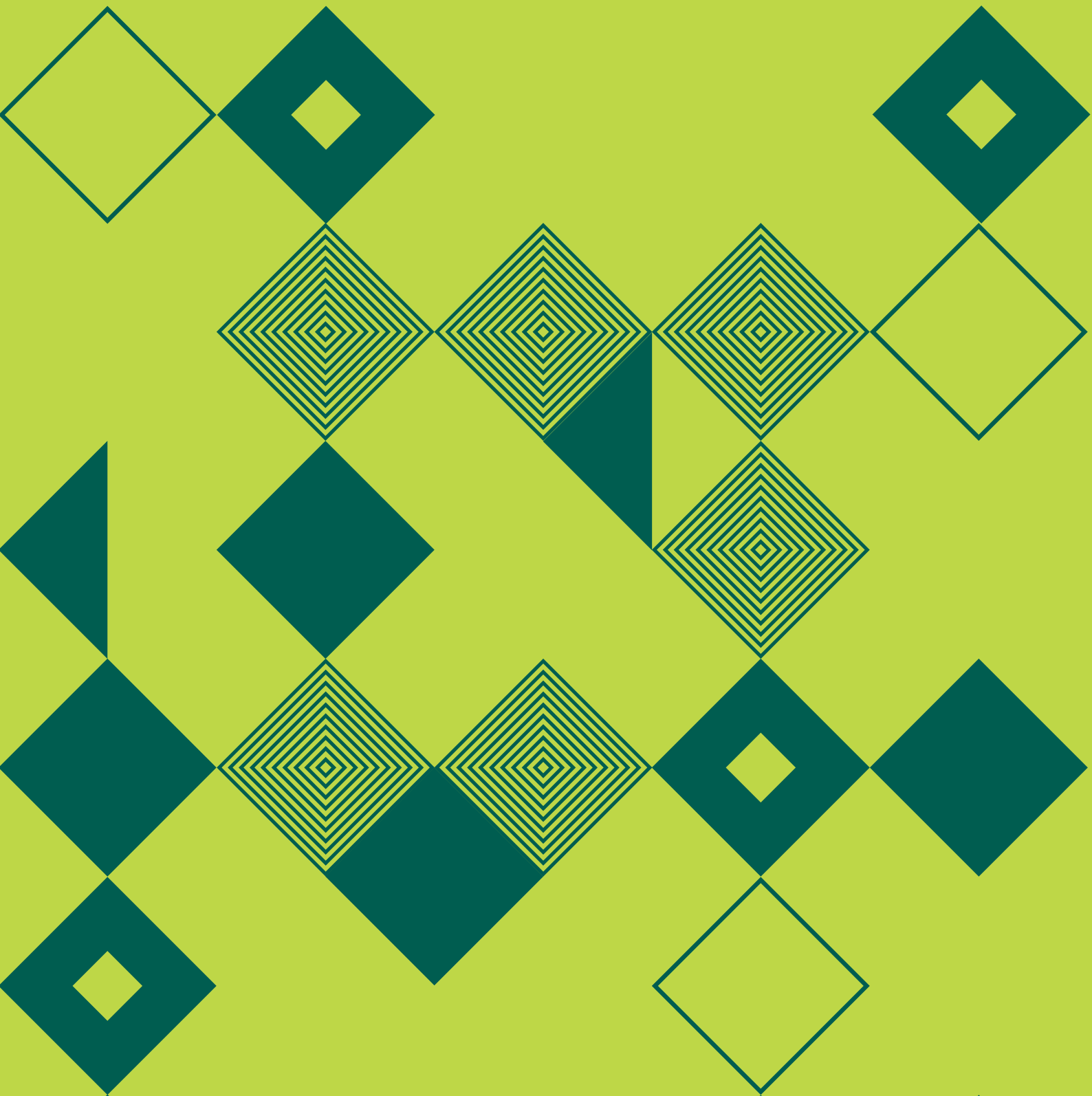


Guidance: Principles of Data Protection



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Foreword



First full year of GDPR

2019 was the first year I heard multiple data protection legal practices say they had found it necessary to hire full-time staff solely to monitor case law and legal developments, such as been the pick-up in developments. If data protection had a big moment in 2018, it has now clearly moved to being an established fixture of public consciousness. From a range of important EU developments including instructive CJEU judgments (such as Fashion ID and Planet49) and the Advocate General's opinion on the SCCs data transfer litigation, to the world's largest data privacy financial penalty (the \$5bn imposed by the FTC on Facebook), it wasn't a year that was short on big news.

Away from the higher profile headlines, it's been the first full calendar year of the operation of the GDPR and the Law Enforcement Directive and many organisations have been quietly getting on with embedding more accountable data practices across their organisations. In Ireland, 1,500 data protection officers (DPOs) have been notified to the DPC and they are engaged daily within public sector and large data processing organisations ensuring data subjects' rights are considered in all projects. DPOs tell us they are keen for more resources and support from the DPC and the DPC will host its first DPO Network conference in Dublin in March 2020. Calls for the provision of more guidance from data protection authorities (DPAs) has been something of a theme during 2019. In June, I participated in a useful stock-taking event in Brussels organised by the EU Commission to mark one year of GDPR and a key takeaway was that across Europe, smaller SMEs are asking for more help to identify reasonable and appropriate implementation measures and for more of a sectoral focus with guidance. The DPC is now engaged in an EU-funded project on awareness raising for SMEs, in cooperation with the Croatian Data Protection Authority, which will assist in driving this forward.

Quantity and Quality

Volume was a key word for the DPC in this first full year of GDPR. Page 71 of this report details the record levels of general guidance the DPC issued to help interpretation of the new law. Page 19 details the volume of complaints lodged with us and the number of individual complaints resolved by the office. At least 40% of our resources are devoted to the handling of individual complaints (as opposed to large-scale and more systemic investigations). The larger-scale inquiries are detailed on page 40 and also consume considerable resources. Page 65 shows the amount of travel and international commitment the DPC makes servicing European Data Protection Board meetings in Brussels (87 meetings in 2019) and engaging with global counterparts to find real-world solutions to long entrenched data protection challenges (for example, how to deliver sufficient transparency to users while also being concise). Breaches notified and individually dealt with by the DPC are set out on page 36. Media queries

responded to and media, conference and parliamentary committee engagements are detailed on page 71. With automated personal data processing in particular now as ubiquitous as blinking and, with hundreds of thousands of processing entities under the supervision of each DPA, the volume of activity is only going to grow.

Disputes between employees and employers or former employers remain a significant theme of the complaints lodged with the DPC, with the battle often staged around a disputed access request. Litigation by individuals against DPC decisions that their data protection rights were not in fact breached at all make up a significant proportion of the litigation the DPC is subject to in the courts today. This is undoubtedly driven by the fact that neither the Workplace Relations Commission nor the Labour Court can order discovery in employment claims, which makes reliance on access requests as adjudicated on by the DPC central to many of these cases. Telcos and banks remain among the most complained about sectors to the DPC, with complaints essentially focussing on account administration and charges. Given these are heavily regulated sectors in Ireland, it is disappointing that more of what are at their core consumer protection issues cannot be sorted out within those sectors, without the need for consumers to lodge complaints with the DPC as a means of being heard. Complaints against internet platforms have also grown in volume, with the main issues centring around management of individuals' accounts and in particular their rights to data erasure when they leave a platform.

In preparation for our pending 5-year regulatory strategy for 2020 to 2025, the DPC engaged in 2019 in focus groups with the public to establish their awareness and expectations of the data protection authority. Key findings are that many people feel confused about their rights with regard to their personal data and would welcome more worked-through scenarios from the DPC, to better understand their application in the real-world. The DPC intends to increase its efforts to produce more case studies and to draw out the lessons from a consumer point of view, as well as that of the controller. What is really encouraging is that people are broadly aware of their rights under GDPR and keen to know how to exercise them.

E-privacy prosecutions for direct marketing offences were pursued rigorously by the office in 2019 and are detailed on page 28. In the meantime, the EU legislature continues to try to conclude a modernised e-privacy regulation to harmonise EU laws on privacy of communications, cookies and direct marketing.

The DPC also completed its consultation on children's personal data and is now preparing to publish guiding principles for controllers. Throughout 2019, the DPC engaged heavily with expert stakeholders in the area of children's digital rights and will continue to work with these parties as we encourage big tech platforms to sign up to a code of conduct on children's data processing.

Creating a larger team and driving forward

To manage the increased volumes of work, the DPC has continued to hire additional staff, increasing our staff numbers from 110 at the start of the year to 140 at the end of 2019. Regulatory lawyers, legal researchers, investigators and technologists all joined the DPC team last year. The ongoing dialogue the DPC maintains with the broad and international community on data protection matters remains an important facet of our role in driving better solutions to both old and newly emerging data protection challenges. In 2019, the DPC was honoured to have been visited by the Commissioners from New Zealand, Australia, Iceland, and the UK, as well as teams of staff from the Swedish, Dutch, Icelandic, Luxembourg and Regional German DPAs. In addition, the DPC hosted study visits by a group of US Congress staffers studying lessons from the GDPR in the context of a potential US Federal Privacy Bill and Californian State Senators examining the issues of technology and data protection.

In 2019, the DPC concluded its first investigation and decision under the new Irish Data Protection Act 2018 (the 2018 Act) and specifically under its provisions that transpose the law enforcement directive. The case concerned the deployment of CCTV and Automatic Number Plate Recognition by An Garda Síochána and a range of corrective powers were exercised by the DPC to drive compliance. A number of other linked investigations into the deployment of surveillance technologies by Local Authorities in Ireland is underway and once the first of these conclude, the DPC intends to publish guidance based on the findings to better ensure all State authorities understand the requirements of the 2018 Act and that the public understand how their rights are protected.

The DPC concluded a detailed investigation into the personal data processing elements of Ireland's national Public Services Card and published its findings in August 2019. These included a finding that there is no lawful basis for the mandating of registration for a Public Services Card by organisations other than by the Department of Employment Affairs and Social Protection when issuing welfare payments. The Department rejected the DPC's findings. The DPC issued an Enforcement Notice and an appeal by the Department to the Circuit Court was lodged before the end of 2019.

A number of other appeals were heard in challenges to decisions of the DPC during 2019 and the decision of the DPC was upheld in each case, as detailed on page 53.

Investigations into big tech companies continued to progress in 2019 with the first two inquiries moving from the investigative stage to the decision-making phase. Much

has been made of the fact that across the EU only three relatively minor cross-border cases have so far resulted in fines, and very modest in size at that, since 25th May 2018 up to the end of 2019. A new legal framework and one that contemplates very significant penalties, not to mention legal novelty in terms of the 'cooperation and consistency' provisions set down, is always going to take time to implement correctly. But have no doubt that intensive work is underway. We currently have: 30 live litigation cases as of the end of 2019; a large-scale and complex investigation into Facebook's transfers of personal data; an appealed Enforcement Notice by the Department of Employment Affairs and Social Protection in Ireland regarding the Public Services Card; further pending e-privacy prosecutions; new corrective powers under the 2018 Act exercised with certain controllers; progress and resolution of thousands of complaints resolved through driving compliance with controllers in 2019. There is certainly no shortage of commitment and capability at the Irish DPC. But equally there is a keen awareness of the legal requirement to apply fair procedures and what it takes to bring cases over the line and the DPC remains focussed on this job. As we have consistently said, there would be little benefit in mass producing decisions only to have them overturned by the courts. When EU competition law rules were first introduced in 1962, it was a further number of years before the first significant decision in the Grundig case issued and a number of years beyond that again before the first fine was issued. Equally, EU competition investigations (and I mention competition law because the fining regime in the GDPR is based on EU competition law) on average take a number of years to complete. As a responsible regulatory body, we are wary of demands for quick-fix solutions and calls for the summary imposition of heavy penalties on organisations for data protection infringements, at least some of which may be based on the application of principles on which there is not always consensus. While acknowledging that the administrative fines mechanism represents an important element of the drive toward the kind of meaningful accountability heralded by the GDPR, we must also recognise that, like any other part of our laws, data protection principles operate within a broader legal context and so, for example, the application and enforcement of such principles by a statutory regulator will always be subject to the due process requirements mandated by our constitutional laws and by EU law. These are constraints that cannot (and should not) be set to one side in some arbitrary fashion or for the sake of expediency.

Brexit

Preparations for “Brexit” have been a considerable body of work for the DPC in 2019 given the implications for what would become restricted personal data transfers to a non-EU country. The DPC issued guidance to help organisations to prepare for both “deal” and “no-deal” scenarios, gave talks at a large number of sectoral events on the issues, provided feedback and direction to a number of government departments and agencies on legal arrangements to cover a no-deal scenario and dealt with a range of organisations seeking to create a main establishment and arrange oversight of their Binding Corporate Rules in Ireland rather than the UK.

unnecessarily privacy invasive data practices and technologies. The Irish DPC is going to continue to be part of the solution using its full range of powers and to contribute to the dialogue and the harnessing of expertise from all quarters to find a better pathway forward.



Helen Dixon
Commissioner for Data Protection

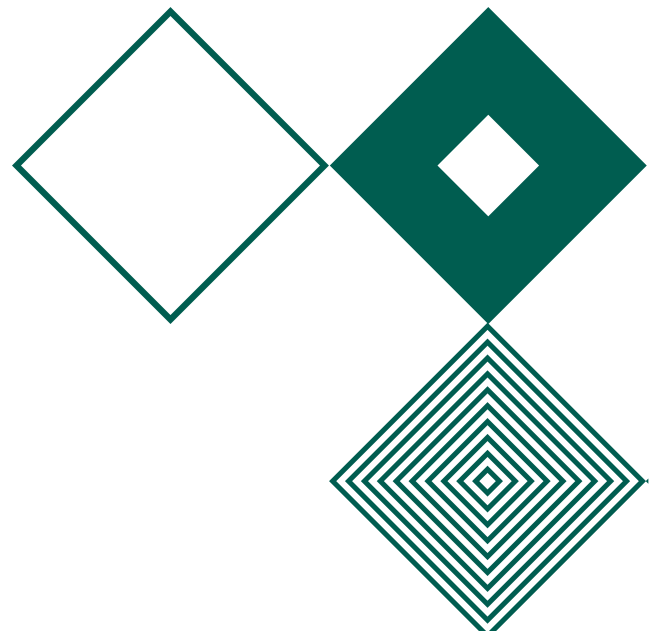
Sad goodbyes

No look-back at 2019 could avoid the sad reminder of the passing of the then European Data Protection Supervisor, Giovanni Buttarelli, in August 2019. The enormous tributes paid to him recognise that he was a giant of a person and a giant of a leader in our community and he is very much missed. Expert counsel for the DPC in many appeal, judicial review and CJEU reference matters, Paul Anthony McDermott, very sadly also passed away in December 2019 and his outstanding achievements and contribution have been rightly well documented in Ireland. Closer to home, an esteemed colleague at the DPC in Ireland, Mark Mullin, passed away during the summer of 2019 and his exceptional contribution, work ethic and fun personality are missed by all of us at the DPC.



Outlook 2020

I am privileged to work with a team that are genuinely excited about the work the DPC does, what we are currently delivering and what we will deliver in the future. These are professionals who work for the DPC because they believe deeply in data protection rights. 2020 is going to be an important year. We await the judgment of the CJEU in the SCCs data transfer case; the first draft decisions on big tech investigations will be brought by the DPC through the consultation process with other EU data protection authorities, and academics and the media will continue the outstanding work they are doing in shining a spotlight on poor personal data practices. The DPC hopes it can create the space to move off “first principles” of GDPR (lawful basis, controller/processor) and really move into the meat of “data protection by design”, to ensure the next generation of technologies we all use does not suffer from the problems we sleep-walked into over the last two decades. We aim by the end of 2020 to have facilitated the progression of big tech towards a code of conduct to better protect children online. The drive in the US to implement more and more privacy legislation is a sign that “enough is now enough” in terms of tolerating



1

Roles and Responsibilities



This is the second annual report of the Data Protection Commission. It has been prepared in accordance with Section 24 of the Data Protection Act 2018 and covers the period from 01 January 2019 to 31 December 2019.

Functions of the DPC

The DPC is the national independent authority in Ireland responsible for upholding the fundamental right of individuals in the European Union (EU) to have their personal data protected. Accordingly, the DPC is the Irish supervisory authority responsible for monitoring the application of the 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 control and process personal data;
- handling complaints from individuals in relation to the potential infringement of their data protection rights;
- conducting inquiries and investigations regarding potential infringements of data protection legislation;
- promoting awareness among organisations and the public of the risks, rules, safeguards and rights in relation to processing of personal data; and
- co-operating with data protection authorities in other EU member states on issues, such as complaints and alleged infringements 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).

Although the DPC regulates under the GDPR and Data Protection Act 2018 in respect of the majority of (non-law enforcement) personal data processing operations carried out from 25 May 2018 onwards, it continues to perform its regulatory functions under the Data Protection Acts 1988 and 2003 in respect of complaints and investigations into potential infringements that relate to the period before 25 May 2018, as well as in relation to complaints and potential infringements that relate 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.

Our SMC comprises:

- Ms Helen Dixon (Commissioner for Data Protection);
- Ms Anna Morgan (Deputy Commissioner — Head of Legal);
- Mr Colum Walsh (Deputy Commissioner — Head of Regulatory Activity);
- Mr Dale Sunderland (Deputy Commissioner — Head of Regulatory Activity);
- Mr Graham Doyle (Deputy Commissioner — Head of Corporate Affairs, Media & Communications);
- Ms Jennifer O'Sullivan (Deputy Commissioner — Head of Strategy, Operations & International);
- Mr John O'Dwyer (Deputy Commissioner — Head of Regulatory Activity); and
- Mr Tony Delaney (Deputy Commissioner — Head of Regulatory Activity).

Funding and Administration

The DPC is funded entirely from the Exchequer, to fulfil its mandate as the independent supervisory body in Ireland for the upholding of data protection rights. In 2019, the DPC welcomed an increased budget allocation of €3.5 million, bringing its total allocation to €15.2 million for the year and this allocation of funding was provided on a full-year basis. The increased funding for the year enabled the DPC to continue to grow its staff complement, from 110 at the start of the year to 140 at 31 December 2019.

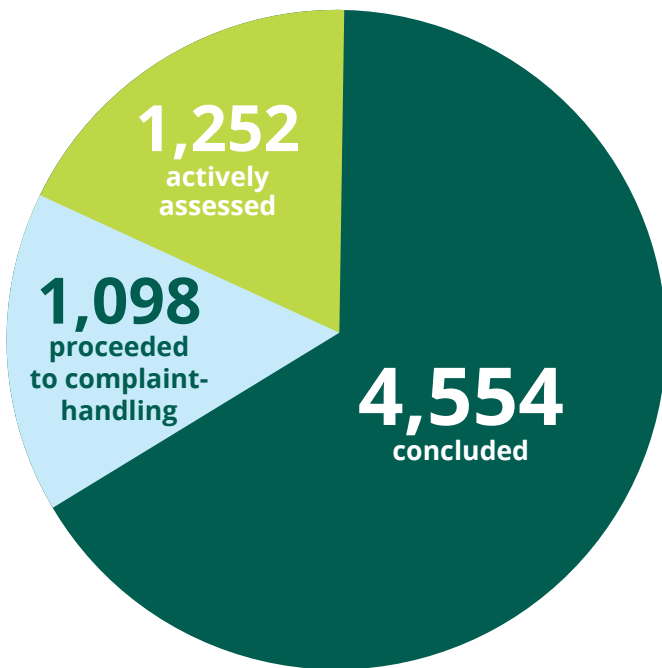
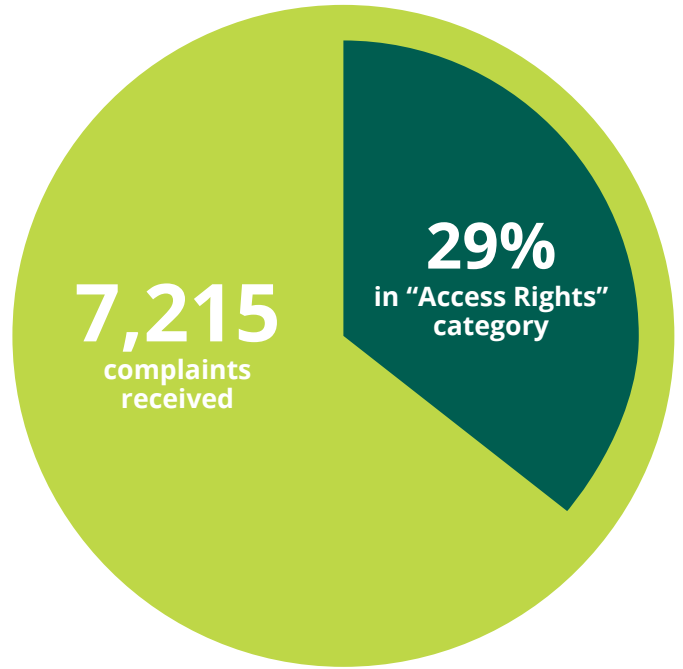
The DPC is preparing its financial statements for 2019. The Financial Statement in respect of the period covered by this report will be appended following the conduct of an audit by the Comptroller and Auditor General.

2

Review of 2019

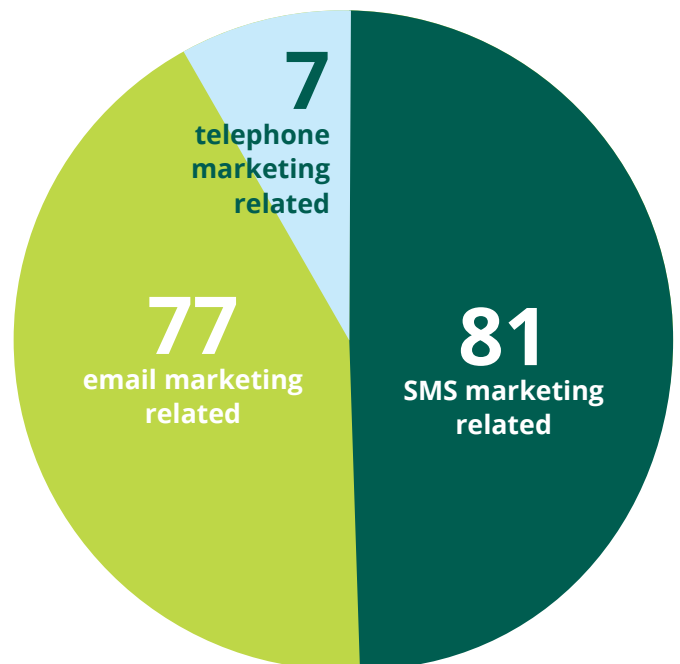


- Total Complaints received was **7,215**, with the largest single category being “Access Rights”, counting for 29% of total complaints received.
- **6,904** complaints were dealt with under GDPR and 311 complaints under the Data Protection Acts 1988 and 2003.



- Of the **6,904** GDPR-related complaints received, **1,252** complaints were actively being assessed on 31 December 2019, **1,098** complaints had proceeded to complaint-handling and **4,554** had been concluded.
- **5,496** complaints in total were concluded in 2019 and the DPC had 2,582 complaints on hand at year-end.
- **620** complaints were also concluded under the Data Protection Acts 1988 and 2003.

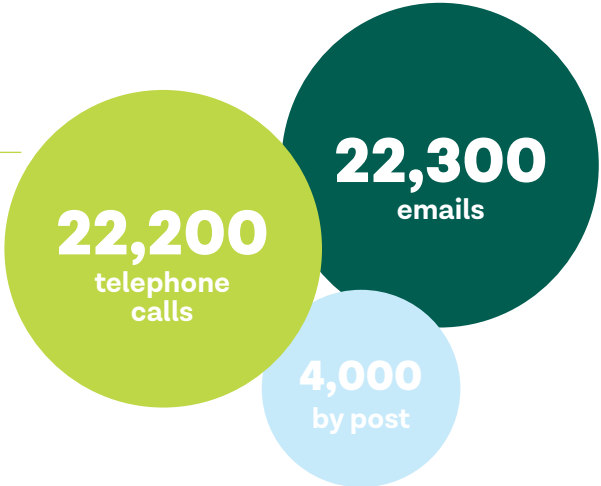
- The DPC issued **29** Section 10 statutory decisions under the Data Protection Acts 1988 & 2003. Of these, **13** fully upheld the complaint, **7** rejected the complaint and **9** partially upheld the complaint.
- **165** new complaints were investigated under S.I. 336 of 2011 in respect of various forms of electronic direct marketing: **77** related to email marketing; **81** related to SMS (text message) marketing; and **7** related to telephone marketing.
- A number of these investigations concluded with successful District Court prosecutions by the DPC. Prosecutions were concluded against **4** entities in respect of a total of **9** offences under the E-Privacy Regulations.



- **457** cross-border processing complaints were received by the DPC through the One-Stop-Shop mechanism that were lodged by individuals with other EU data protection authorities.
- **207** data-breach complaints were handled by the DPC from affected individuals.
- **6,069** valid data security breaches were recorded, with the largest single category being “Unauthorised Disclosures”.



- Information and Assessment received almost **48,500** contacts comprising approximately **22,300** emails, **22,200** telephone calls and almost **4,000** items of correspondence via post.
- **6** statutory inquiries were opened in relation to multinational technology companies' compliance with the GDPR, bringing the total number to **21**.



- The number of general consultation queries received was **1,420**.



- The DPC was lead reviewer in 19 Binding Corporate Rules (BCRs) applications
- DPC staff spoke or presented at over **180** events, including conferences, seminars, and presentations to individual organisations from a broad range of sectors.

Spoke and presented
at events on over

180
occasions

- The DPC expanded its social media activities across Twitter, LinkedIn and Instagram, and at year-end had a combined followership of over **20,000** and an organic monthly reach in the hundreds of thousands.
- The DPC carried out an extensive consultation on the processing of children's personal data, yielding **80** responses and the results of that consultation will feed into the development of guidance on processing children's data, which is a DPC priority for 2020.
- Work on the DPC's new Regulatory Strategy continued with a consultation document on the DPC's Target Outcomes and focus groups with individuals.
- The DPC published its findings on certain aspects of the Public Services Card ("PSC") following a lengthy investigation. The published findings were targeted at two key issues, namely the legal basis under which personal data is processed and transparency.
- An appeal to the Dublin Circuit Court against the enforcement notice was issued in late 2019 by the Minister for Employment Affairs and Social Protection and this appeal is listed to come before the Court for the first time in March 2020.
- The DPC received **712** Data Protection Officer notifications, bringing the number to **1,596**.

20,000
followers

712

Data Protection
Officer
notifications

3

Information and Assessment

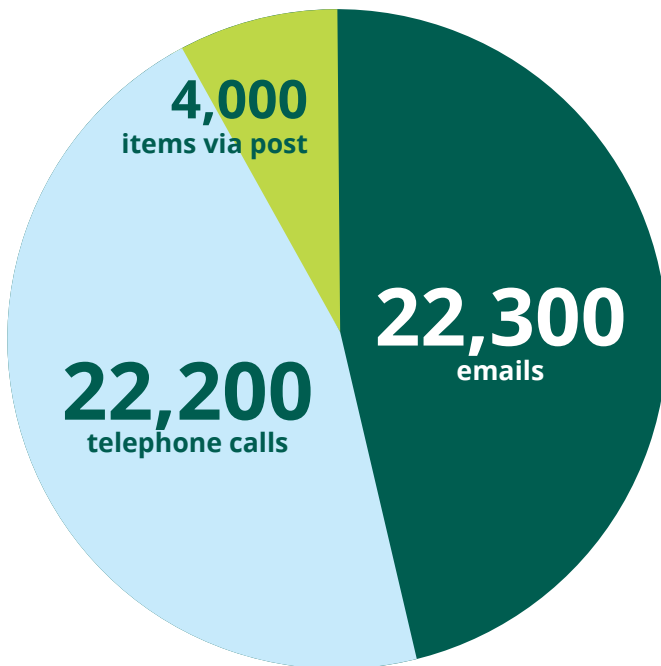


A key objective of the DPC is to provide a responsive and high-quality information service to individuals and organisations regarding their rights and responsibilities under data protection legislation.

Information and Assessment at the DPC provides a public-information helpdesk service, and receives and responds to queries from individuals and organisations by means of email, online form or telephone. In addition, it carries out early-stage assessment, determining whether a communication needs to be escalated within the DPC and the most appropriate route for doing so.

Responding to Queries and Complaints

In the first full calendar year of the GDPR, the DPC continued to deal with a significant number of contacts from individuals and organisations. In 2019, the DPC received almost 48,500 contacts comprising approximately 22,300 emails, 22,200 telephone calls and almost 4,000 items of correspondence via post.



In order to provide an efficient service, the DPC continues to look at its processes with a view to delivering greater efficiencies for all users. Enhancing the quality and responsiveness of the service provided by the DPC will continue to be a priority in 2020.

Emerging Trends and Patterns

The DPC, through analysis of the issues brought to its attention, also identifies emerging trends and patterns that are of concern to individuals and organisations. This helps the DPC to focus its external communications on the most pertinent issues and will help guide the DPC's communications throughout 2020.

Topics of particular interest where the DPC provided support to individuals during the year included:

- individual concerns relating to the role and use of the Public Services Card;
- the use of CCTV — particularly in the context of neighbour disputes and the application of the domestic exemption;
- access requests on behalf of children — queries from both individuals and organisations seeking clarification as to how they should respond accurately, appropriately and in the child's best interests;
- where is my data? — requests relating to medical practices that have closed (often where a practitioner has died) and patients are unable to establish who is now in control of their personal data;
- HR/employment disputes — specifically workplace surveillance but also concerns about sharing of information in the context of those disputes and the redaction of third party data in response to employee access requests;
- exam information — in particular queries relating to examiner's notes; and
- photography — Particularly as it relates to consent, publication and artistic exemptions.

4 Complaints



How Complaints are handled

Since the application of the GDPR, the DPC has seen a significant increase in the number of complaints received. This trend continued in the first full calendar year of the application of the GDPR. In 2019, 7,215 complaints were received by the DPC.

The DPC processes complaints received under two main legal frameworks during this period:

- complaints received from 25 May 2018 onwards are dealt with under the GDPR, Law Enforcement Directive, and the provisions of 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.

The term “complaint” has a very specific meaning under the GDPR (and the LED) and the provisions of the Data Protection 2018 that implement those laws.

For a communication to constitute a complaint — and therefore trigger the DPC’s particular statutory complaint-handling obligations — it must fall under one of the following categories:

- a complaint from an individual relating to the processing of their own personal data;

- a legally authorised entity complaining on behalf of an individual; and
- advocacy groups acting as permitted within the parameters laid out in the GDPR, LED and the Data Protection Act 2018.

During the complaint-handling process the DPC has an obligation to provide the complainant with progress updates and ultimately inform the individual of the outcome of the complaint. The DPC issues updates to complainants every three months in accordance with its obligations.

Of the 7,215 complaints received by the DPC, 6,904 were GDPR complaints, while 311 were complaints handled under the Data Protection Acts 1988 to 2003.

As in previous years, the category of Access Requests was the highest complaint-type received by the DPC between in 2019 (29%), though in proportion to overall complaints it is dropping. Complaints relating to Unfair Processing of Data (16%) and Disclosure (19%) were also once again received in high volumes.

In 2019, the Commissioner issued 29 decisions under the Data Protection Acts 1988 & 2003. Of these, 13 fully upheld the complaint, 7 rejected the complaint and 9 partially upheld the complaint.

Complaints received under the GDPR

Note: the top five complaints represent 76% of total complaints received.

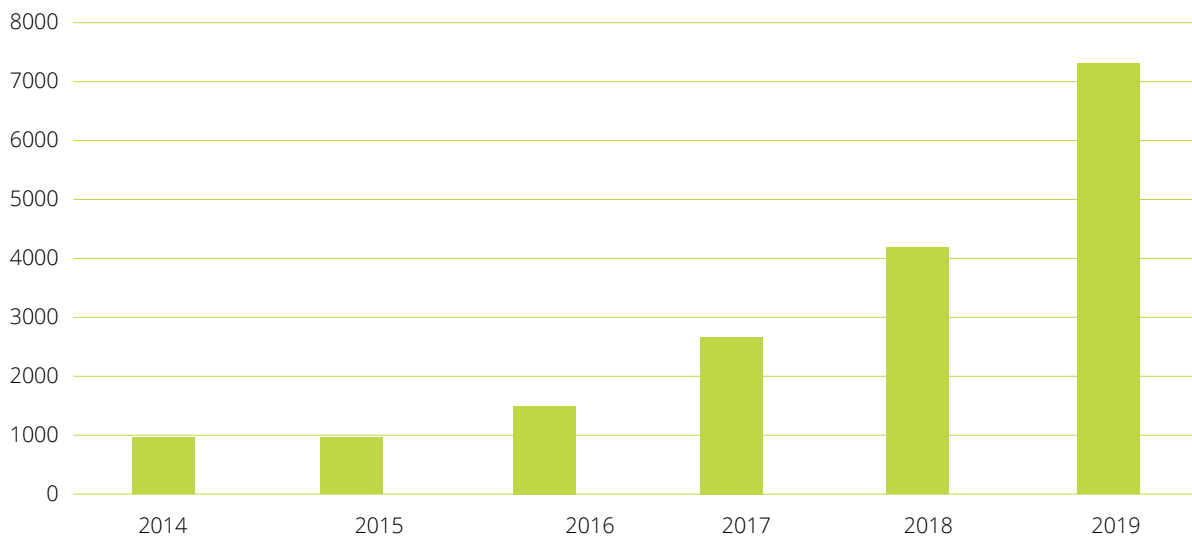
Complaints Received During 2019 — Top 5 Categories of Complaints	No	% of total
Access Request	1,971	29%
Disclosure	1,320	19%
Fair Processing	1,074	16%
e Marketing Complaints	532	8%
Right to erasure	353	5%

Complaints received under the 1988 & 2003 Acts

Note: the top 5 represents 83% of total complaints received.

Complaints Received During 2019 — Top 5 Categories of Complaints	No	% of total
Access Request	93	30%
Fair Processing	87	28%
Disclosure	57	18%
Fair Obtaining	13	4%
Specified Purpose	9	3%

Complaints received 2014–2019



Complaint case studies

under the Data Protection Act 2018

CASE STUDY 1

Right to rectification request to a healthcare group (Applicable Law — GDPR & Data Protection Act 2018)

We received a complaint against a healthcare group arising from its refusal of a request for rectification under Article 16 of the GDPR. The complainant alleged that the healthcare group was incorrectly spelling his name on its computer system by not including the síneadh fada, an accent that forms part of the written Irish language.

Hospitals under the administration of this healthcare group use a patient administration system to initially record patient data which is then shared with other systems at later points of patient care, i.e. Laboratory, Radiology and Cardiology. The healthcare group informed the complainant that it is not possible to record the síneadh fada because syntax characters are recorded as commands on the PAS, impacting on the way data is stored and processed.

The healthcare group informed the DPC that the patient administration system is due to be replaced in 2019/2020. However, the group's new system will not allow for the use of the síneadh fada. The healthcare group informed the DPC this was for the purpose of enabling a streamlined single point of contact for patient information across different systems. This would enable professionals to access this information across different units within a hospital or hospital group without re-entering the data at a later point, thereby avoiding potential for later errors. The other systems across the current healthcare group network and/or wider hospital network do not support the use of the síneadh fada. The healthcare group further advised the DPC that they identify patients with Patient ID numbers rather than isolated names.

The DPC examined this submission and concluded that any update of the computer system would lead to costs in terms of significant costs and time, along with errors in storage and matching of records. The DPC also engaged with An Coimisinéir Teanga (Irish Language Regulator) about its advice to public sector organisations with respect to computer systems supporting the síneadh fada. An Coimisinéir Teanga advised there is no such obligation arising from the Official Languages Act 2003 but such an obligation can arise from a language scheme — an agree-

ment put in place between a public body and the Minister for Culture, Heritage and the Gaeltacht.

The DPC queried the healthcare group on the existence of a language scheme and was provided a copy. This scheme sets out a respect for patient choices regarding names, addresses and their language of choice. The scheme also provides a commitment to update computer systems to achieve "language compliancy". There is no timeframe provided for the fulfilment of this commitment in the language scheme.

The healthcare group advised the DPC they are committed to patient safety as a primary, core concern and further advised the DPC of the difficulties associated with sharing and storing information across other systems if they updated their system to allow for the use of the síneadh fada. They also advised that they will be testing the possibility of using the síneadh fada in any update of their computer system.

The DPC had regard to Article 16 and Article 5(1) (d) of the GDPR in examining this complaint. Both articles set out the rights of individuals subject to "the purposes of the processing". The right to rectification under Article 16 of the GDPR is not an absolute right. Organisations that control or process personal data are required to take reasonable steps in the circumstances. The DPC had regard to case law from the European Court of Human Rights on linguistic rights and/or naming. This case law reflects that the spelling of names falls under the ambit of Article 8 of the European Convention on Human Rights but that the Court adopts a restrictive approach in this regard. As such, the DPC reiterated the purpose of the processing in the circumstances of the complaint was the administration of health care to the complainant and involved the use of Patient ID numbers. The name of the complainant

was not the isolated means of identification and therefore the purpose of the processing is being achieved without the use of diacritical marks.

The DPC had regard to any risks to the complainant in the refusal of their Article 16 request also. The DPC noted the risk to the complainant would increase because of the difficulties associated with cross-system handling of the síneadh fada and the impact this would have on any health care decision making for the individual. In the circumstances, the non-use of the síneadh fada would not constitute an interference with the fundamental rights of the individual.

Under section 109(5) (f) of the Data Protection Act 2018 (the 2018 Act), the DPC requested the healthcare group to inform the complainant of its actions in the implementation of a computer system enabled to reflect the síneadh fada. Also, the DPC requested that the group add an addendum to the individual's file to show the síneadh fada forms part of the individual's name.

The DPC, under section 109(5)(c) of the 2018 Act, advised the complainant that he may contact An Coimisinéir Teanga about the language scheme and any contravention of same.

Complaint case studies under the Data Protection Acts 1988 & 2003

CASE STUDY 2

Unauthorised disclosure of mobile phone e-billing records, containing personal data, by a telecommunications company, to the data subject's former employer

(Applicable law: Data Protection Acts 1988 and 2003 ("the Acts"))

Background

The complainant, during a previous employment, asked the telecommunications company to link her personal mobile phone number to her (then) employer's account. This enabled the complainant to avail of a discount associated with her (then). While this step resulted in the name on the complainant's account changing to that of her (then) employer, the complainant's home address remained associated with the account and the complainant remained responsible for payment of any bills.

Following termination of the employment relationship, the complainant contacted the telecommunications company to ask that it (i) restrict her former employer's access to her mobile phone records; and (ii) separate the account from that of her former employer. Following this request, an account manager took a number of steps in the mistaken belief that this would result in the separation of the complainant's account from that of her former employer. The complainant, however, became aware that, subsequent to her request, her former employer continued to access her account records. On foot of further inquiries from the complainant, the telecommunications company discovered its error and the complainant's account was eventually separated from that of her former employer.

The complainant subsequently submitted a complaint to the telecommunications company. Having investigated the complaint, the company informed the complainant that it did not have a record of the original account restriction request. In the circumstances, the complainant referred a complaint to this office.

Investigation

During our investigation, the telecommunications company acknowledged that the initial action taken by its account manager was insufficient as it did not separate the complainant's account from that of her former employer and neither did it prevent her former employer from accessing her e-billing records. The company further

acknowledged that its records were incomplete when it investigated the complainant's complaint. It confirmed, in this regard, that it had since located the complainant's initial restriction/separation request.

The issues for determination, therefore, were whether the telecommunication company, as data controller:

1. implemented appropriate security measures, having regard to Sections 2(1)(d) and 2C(1) of the acts in order to protect the complainant's personal data against unauthorised access by, and disclosure to, a third party (i.e. the complainant's former employer); and
2. kept the complainant's data accurate, complete and up to date, as required by Section 2(1)(b) of the Acts.

Appropriate Security Measures

This office found that the telecommunications company did not implement appropriate security measures to protect the complainant's personal data from unauthorised access by, and disclosure to, her former employer. This was self-evident from the fact that the complainant's former employer continued to access her e-billing records despite the initial actions taken by the telecommunications company.

This office further noted the obligation, set out in Section 2C(2) of the Acts, for a data controller to "... take all reasonable steps to ensure that — (a) persons employed by him or her ... are aware of and comply with the relevant security measures aforesaid ...". This office found that the telecommunications company had not complied with its obligations in this regard. Again, this was self-evident from the fact that the account manager who initially actioned the complainant's request was operating on the mistaken belief that the actions taken were sufficient to achieve separation of the complainant's account from that of her former employer.

Accurate, complete and up to date

This office also considered the fact that, at the time when the complainant referred her complaint to the telecommunications company, the company could not locate her initial account restriction request. The result of this was that the outcome of the company's own investigation into the individual's complaint was incorrect. Accordingly, and notwithstanding the subsequent rectification of the position, this office found that the telecommunications company failed to comply with its obligations under Section 2(1)(b) of the Acts in circumstances where the complainant's records, at the relevant time, were inaccurate, incomplete and not up to date.

Key Takeaways

The above case study highlights the fact that the obligation to keep personal data safe and secure is an ongoing one. Data controllers must ensure that they continuously monitor and assess the effectiveness of their security measures, taking account of the possibility that the circumstances or arrangements surrounding its data processing activities may change from time to time. In this case, the data controller failed to take the required action to reflect the change in circumstances that was notified to it by the complainant when she requested the restriction and separation of her account from that of her former employer. The case study further highlights the importance of effective training for employees in relation to any internal protocols.

CASE STUDY 3

Reliance on consent in the use of child's photograph in the form of promotional material by a State Agency

(Applicable law — Data Protection Acts 1988 and 2003)

We received a complaint from a parent in respect of their child. The parent had attended a festival organised by a state agency with their child, where a professional photographer took the child's photograph. The following year the state agency used this photograph in promotional material. The child's parent, while accepting that they had conversed with the photographer, had understood at the time of the photograph that they would be contacted prior to any use of the image.

During the investigation, the state agency indicated that they had relied upon consent pursuant to section 2A(1) (a) of the Acts as the photographer had obtained verbal permission from the child's parent. However, the state agency also accepted that it was not clear to the child's parent that the image would be used for media/PR purposes. The state agency further accepted that the parent was not adequately informed regarding the retention of

the image. The DPC welcomed the state agency's indications that it would immediately review their practices and procedures.

In conclusion, the DPC found that the state agency had not provided the child's parent with adequate information in order to consent to the processing of the image used in promotional material.

CASE STUDY 4

Receivers and fair processing

We received a complaint against a private receiver who was appointed by a financial institution over the complainant's property.

The complaint alleged infringements of the Acts on the basis that the receiver:

- was not registered as a controller pursuant to section 16 of the Acts;
- had no lawful basis for obtaining the complainant's personal data from the financial institution;
- further processed personal data unlawfully by disclosing information to a company appointed by the receiver to manage the receivership (the receiver's "managing agent");
- opened a bank account in the complainant's name;
- obtained the property ID and PIN from Revenue which gave the receiver access to the complainant's personal online Revenue account; and
- insured the property in the complainant's name.

Following an investigation pursuant to section 10 of the Acts, the DPC established that the receiver was appointed by the financial institution on foot of a Deed of Appointment of Receiver (DOA) which granted the receiver powers pursuant to the Conveyancing Act 1881, and pursuant to the mortgage deed between the complainant and the financial institution. On being appointed, the receiver wrote to the complainant informing them of their appointment as the receiver over the complainant's property and provided a copy of the DOA. The receiver appointed a separate company as their managing agent to assist in the managing of the property. During the receivership, the receiver liaised with Revenue in order to pay any outstanding taxes on the property, such as the Local Property Tax (LPT). It was also established that the receiver opened a bank account for the purpose of managing the income from the property. The bank account name included the name of the complainant. It was further established that an insurance policy was taken out, in respect of the property. This insurance policy referred to the complainant's name.

The DPC first considered whether a receiver was required to register as a data controller in accordance with section 16 the Acts, and whether the exemptions listed in the Data Protection Act 1988 (Section 16(1)) Regulations 2007 (the "Registration Regulations") applied. The DPC held that a receiver was not required to register, as the exemption under regulation 3(1)(g) of the Registration Regulations applied to the receiver. Regulation 3(1)(g) exempted data controllers who were processing data in relation to its customers. Having considered the relationship between the complainant and the receiver, the DPC held that the exemption applied in respect of the receiver's activities regarding the complainant.

Next the DPC considered whether the receiver had a lawful basis for obtaining the personal data from the financial institution, disclosing it to the managing agent, and whether such processing constituted further processing incompatible with the original purpose it was obtained pursuant to section 2(1)(c)(ii) of the Acts. The complainant had a mortgage with the financial institution which had fallen into arrears. Under section 19(1)(ii) of the Conveyancing Act 1881, the financial institution could appoint a receiver once the debt on the mortgage had come due. Section 2A(1)(b)(i) of the Acts permits processing of personal data where the processing is necessary "for the performance of a contract to which the data subject is party". The mortgage deed was a contract between the data subject and the financial institution, and in circumstances where the terms of the contract were not being adhered to, the appointment of the receiver by the financial institution was necessary for the performance of the contract. The DPC held that the receiver had a lawful basis for obtaining the complainant's personal data from the financial institution.

The DPC also found that the receiver had a lawful basis pursuant to section 2A(1)(b)(i) of the Acts to disclose personal data to its managing agent, to assist in the day to day managing of the receivership. The DPC found that the financial institution obtained the complainant's personal data for the purposes of entering into a loan agreement. This was specific, explicit and a legitimate purpose. The disclosure of the complainant's personal data by the financial institution to the receiver, and by the receiver to the managing agent was in accordance with the initial purpose for which the personal data was obtained. This processing during the receivership did not constitute further processing pursuant to section 2(1)(c)(ii) of the Acts.

The DPC assessed whether the receiver had a lawful basis to open a bank account in the complainant's name. The complainant submitted that this account was opened without their knowledge or consent. Consent is one of the lawful bases for processing personal data under the Acts. The DPC considered whether the receiver otherwise had a lawful basis for processing under section 2A(1)(d) of the Acts, on the basis of legitimate interests. To assess this lawful basis, the DPC took account of the Court of Justice of the European Union (CJEU) case in *Rīgas C-13/16*¹ which sets out a three step test for processing on the basis of legitimate interests, as follows:

1 Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' Case C-13/16

- the processing of personal data must be for the pursuit of a legitimate interest of the controller or a third party;
- the processing must be necessary for the purpose and legitimate interests pursued; and
- the fundamental rights and freedoms of the individual concerned do not take precedence.

The DPC held that the opening of the bank account was a reasonable measure to manage the income and expenditure during a receivership. The receiver submitted that referring to complainant's name as part of the bank account name was necessary to ensure the receivership was carried out efficiently and to avoid confusion between different receiverships. While it would have been possible to open an account without using the complainant's name, the DPC took account of the CJEU's judgment in *Huber v Bundesrepublik C-524/06*² where the Court held that processing could be considered necessary where it allowed the relevant objective to be more effectively achieved. The DPC held that the reference to the complainant's name on the bank account was therefore necessary, as it allowed for the more effective pursuit of the receiver's legitimate interests.

With regard the third element of the legitimate interests test (which requires a balancing exercise, taking into account the fundamental rights and freedoms of the data subject) the DPC held that the reference to the complainant's name on the account would have identified them to individuals who had access to the bank account or been supplied with the bank account name. The DPC balanced these concerns against the administrative and financial costs which would result from the need for the receiver to implement an alternative procedure for naming accounts. On balance, the DPC did not find that the complainant's fundamental rights took precedence over the legitimate interests of the receiver and as a result, the receiver had a lawful basis for processing the complainant's name, for the purpose of the receiver's legitimate interests.

With regard to the allegation that the receiver had gained access to the personal Revenue account of the complainant, the DPC found that the receiver did not gain access to the complainant's personal online Revenue account as alleged. The receiver was acting as a tax agent in relation to the LPT and this did not allow access to a personal Revenue account. In relation to the insurance policy being taken out in the complainant's name the DPC held that the receiver did not process personal data in this instance.³

During the course of the investigation the DPC also examined whether the receiver had complied with the data protection principles under section 2 of the Acts. In this regard, the DPC examined the initial correspondence the receiver had sent to the complainant notifying them of their appointment. This correspondence consisted of a cover letter and a copy of the DOA. The cover letter and DOA were assessed in order to determine whether the receiver had met their obligation to process the personal data fairly. Section 2D of the Acts required an organisation in control of personal data to provide information on the identity of the data controller, information on the intended purposes for which the data may be processed, the categories of the data concerned as well as any other information necessary to enable fair processing. The DPC held that the correspondence was sufficient in informing the complainant of the identity of the data controller (and original data controller). However, the DPC held that, while a receiver was not required to provide granular information on each purpose for which personal data was to be processed, the receiver should have given a broad outline of the purposes for which the personal data was intended to be processed, and this was not done in this case. It was also held that the receiver should have provided the categories of personal data they held in relation to the complainant, but this was not done. In light of this, the DPC held that the receiver had not complied with section 2D of the Acts.

This decision of the DPC demonstrates that private receivers and their agents may lawfully process personal data of borrowers, where such processing is necessary in order to manage and realise secured assets. Individuals should be aware that their information may be processed without their consent in circumstances where a deed of mortgage provides for the appointment of a receiver. At the same time, receivers must comply with their obligations under the Acts and GDPR to provide individuals with information on processing at the outset of the receivership.

The decision is currently the subject of an appeal by the complainant to the Circuit Court

2 *Heinz Huber v Bundesrepublik Deutschland Case C-524/06*

3 The processing of personal data was considered in a similar case where the same complainant made a complaint against the managing agent in this case. In that decision the DPC held that the managing agent had legitimate interest in processing the complainant's personal data for the purposes of insuring the property

Access Rights Complaints

During 2019, the DPC received 2,064 complaints relating to the right of access, a high proportion of which dealt with the failure of organisations in control of personal data to respond to an access request, or failure to release all the appropriate data on foot of an access request. In 2019 an increased number of complaints received were against banks and solicitors practices, as well as complaints concerning the failure of schools and sporting clubs to respond to access requests.

The GDPR broadens the extent of the subject access right compared with the previous legal framework and this enhanced right was possibly evident in the increased level of applications to the State Examinations Commission in August 2019. An individual has a right to a copy of the personal data which the State Examinations Commission holds and this right of access extends to examination scripts. Whereas previous legislation dealt with the right of access to exam results, Section 56 of the 2018 Act the first time specifically addresses the right of access to scripts of examinations and results of appeal.

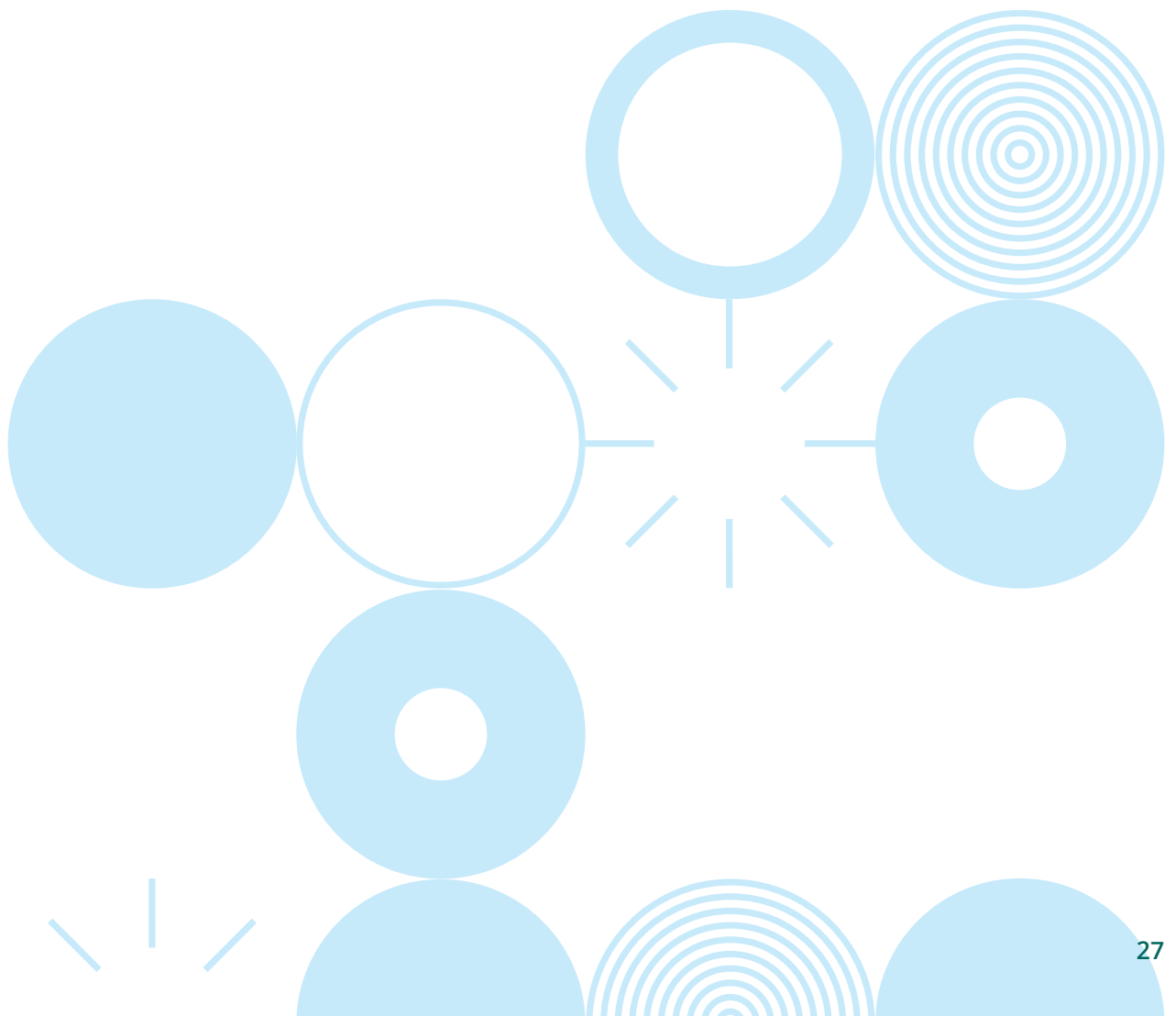
Although an important fundamental right, the right of access is not an absolute right. The GDPR prescribes a mechanism in Article 23 to permit the restrictions of

rights in particular and specific circumstances. This enables member states to introduce their own exemptions in national legislation. In Ireland this has been achieved through Section 60 of the 2018 Act.

Importantly, any restriction relied upon by controllers, must respect the essence of the fundamental rights and freedoms and be a necessary and proportionate measure in a democratic society to safeguard important objectives of general public interest. This issue will be examined by the DPC in any case where exemptions are relied on.

In addition to the restrictions contained in Section 60, Article 15 of the GDPR requires that when responding to an access request, third-party data must be protected and states "The right to obtain a copy in response to an access request shall not adversely affect the rights and freedoms of others including trade secrets or intellectual property and in particular copy right protecting the software".

Upon receipt of an access request, it is important for controllers to remember that the right of access is a fundamental right, so there is a presumption in favour of disclosure on the part of controllers.



Direct Marketing Complaints

The DPC received 165 new complaints in relation to direct electronic marketing in 2019, some 77 in relation to unsolicited email, 81 in relation to unsolicited text messages (SMS) and 7 in relation to unsolicited telephone calls. A number of the complaints related to more than one type of unsolicited marketing from the same organisation.

A total of 130 direct marketing complaint investigations were concluded during the year.

Prosecutions in relation to electronic direct marketing

The DPC prosecuted 4 entities in relation to direct electronic marketing without consent. These included the telecommunications provider Vodafone Ireland Limited, food ordering service Just-Eat Ireland Limited, and online retailers Cari's Closet Limited and Shop Direct Ireland Limited (t/a Littlewoods Ireland).

CASE STUDY 5

Prosecution of Vodafone Ireland Limited

In April 2019 the DPC received two separate complaints from an individual who had received unsolicited direct marketing communications by text and by email from the mobile network operator Vodafone. The individual stated that Vodafone had ignored their customer preference settings, which recorded that they did not wish to receive such marketing.

During our investigation, Vodafone confirmed that the complainant had been opted-out of direct marketing contact but that communications were sent to them due to human error in the case of both the text message and the email marketing campaigns.

In the case of the SMS message, Vodafone confirmed that a text offering recipients the chance to win tickets to an Ireland v France rugby match was sent to approximately 2,436 customers who had previously opted-out of receiving direct marketing by text. This was as a result of a failure to apply a marketing preferences filter to the SMS advertising campaign before it was sent.

In the case of the email received by the complainant, an application that was intended to be used to send direct marketing to prospective customers was used in error and the message was sent to existing Vodafone customers. While Vodafone was unable to definitively confirm the number of customers who were contacted by email contrary to their preference, the marketing email was sent to 29,289 existing Vodafone customers. The company confirmed that some 2,523 out of 7,615 of these were contacted in error. However, it was unable to link the remaining 21,674 customers who were sent the same email with their marketing preferences in Vodafone's data warehouse to confirm the total number contacted in error.

The DPC had also received a separate complaint in February 2019 from another individual who was a former customer of Vodafone. This customer had ceased to be a Vodafone customer more than five years earlier and they still continued to receive promotional text messages. In the course of our investigation, Vodafone confirmed that the direct marketing messages were sent to the complainant in error. It said that in this exceptional case, the complainant's mobile number was not removed from the platform used to send marketing communications when their number was no longer active on the network.

As the DPC had previously prosecuted Vodafone in 2011, 2013 and 2018 in relation to direct electronic marketing offences, we decided to initiate prosecution proceedings in relation to these complaints.

At Dublin Metropolitan District Court on 29 July 2019, Vodafone pleaded guilty to five charges of sending unsolicited direct marketing communications in contravention of S.I. No. 336 of 2011 ('the ePrivacy Regulations'). The company was convicted and fined €1,000 on each of three charges and convicted and fined €750 each in respect of the two remaining charges.

CASE STUDY 6

Prosecution of Just-Eat Ireland Limited

We received a complaint from an individual in November 2018 regarding unsolicited direct marketing emails from Just-Eat Ireland Limited. The complainant had unsubscribed from the company's direct marketing emails but several days later received an unsolicited marketing email. During our investigation of this complaint the company informed us that the complainant's attempt to unsubscribe was unsuccessful due to a technical issue with its email platform. This issue affected 391 customers in Ireland.

As Just-Eat Ireland Limited had previously been warned by the DPC in 2013 on foot of complaints in relation to unsolicited direct marketing emails, we decided to initiate prosecution proceedings.

At Dublin Metropolitan District Court on 29 July 2019, Just-Eat Ireland Limited pleaded guilty to one charge in relation to sending an unsolicited direct marketing email. The court applied section 1(1) of the Probation of Offenders Act in lieu of a conviction and fine on the basis that the company donate €600 to the Peter McVerry Trust charity.

CASE STUDY 7

Prosecution of Cari's Closet Limited

In May 2018, we received a complaint against the online fashion retailer Cari's Closet from an individual who had in the past placed an online order with the company. The complaint concerned the receipt of three unsolicited direct marketing emails. The same person had previously complained to the DPC in January 2018 about unsolicited emails from that company. On that occasion, the complainant said they had received over forty marketing emails in one month alone. The person had attempted, without success, to unsubscribe on a couple of occasions.

Cari's Closet attributed the failure to properly unsubscribe the complainant from emails to a genuine mistake on its behalf.

As the DPC had issued a warning in April 2018 in relation to the earlier complaint, we decided to initiate prosecution proceedings against the company.

At Dublin Metropolitan District Court on 29 July 2019, Cari's Closet pleaded guilty to one charge of sending an unsolicited direct marketing email to the complainant. In lieu of a conviction and fine, the court applied section 1(1) of the Probation of Offenders Act on the basis that the company donate €600 to the Little Flower Penny Dinners charity.

CASE STUDY 8

Prosecution of Shop Direct Ireland Limited t/a Littlewoods Ireland

In May 2019, the DPC received a complaint from an individual who said they had been receiving direct marketing text messages from Littlewoods since March. The complainant stated that they had followed the instructions to unsubscribe by texting the word 'STOP' on five occasions to a designated number known as a short code, but they had not succeeded in opting out and they continued to get marketing text messages.

In the course of our investigations, Shop Direct Ireland Limited (t/a Littlewoods Ireland) confirmed it had a record of the complainant's opt-out from direct marketing texts submitted through their account settings on the Littlewoods website on 8 May 2019. It did not, however, have a record of their attempts to opt-out of direct marketing texts on previous occasions using the SMS short code. This was due to human error in setting up the content for the SMS marketing messages. The company said that the individual responsible for preparing and uploading content relating to marketing texts had mistakenly included the opt-out keyword 'STOP' instead of 'LWISTOP' at the end of the marketing texts.

Shop Direct Ireland Limited had previously been prosecuted by the DPC in 2016 in relation to a similar issue which resulted in a customer attempting, without success,

to unsubscribe from direct marketing emails. On that occasion, the court outcome resulted in the company making a donation of €5,000 to charity in lieu of a conviction and fine.

The DPC decided to prosecute the company in respect of direct electronic marketing offences in relation to the May 2019 complaint.

At Dublin Metropolitan District Court on 29 July 2019, Shop Direct Ireland Limited (t/a Littlewoods Ireland) entered guilty pleas to two charges relating to sending unsolicited direct marketing text messages. The court ruled that the company would be spared a conviction and fine if it donated €2,000 each to the Peter McVerry Trust and the Little Flower Penny Dinners charities and section 1(1) of the Probation of Offenders Act was applied.

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.

The DPC is the Lead Supervisory Authority for a broad range of multinationals, including many large technology and social media companies whose main establishment is located in Ireland and it handles complaints originally lodged with other EEA data protection supervisory authorities, in addition to handling complaints that people lodge directly with the DPC. In the past year, a significant number of complex cross-border complaints were transferred to the DPC by other data protection supervisory authorities. In addition, the DPC continued and commenced several large-scale inquiries that were initiated on the DPC's own volition and that relate to cross-border processing. Although the DPC has primary supervisory responsibility, we must consult extensively with the other data protection supervisory authorities and keep them updated throughout our complaint handling and investigatory processes. In particular, we must take due account of their views and seek their consensus on our draft

decisions on these cross-border cases, under the GDPR's cooperation mechanism.

The role of the lead supervisory authority (LSA) includes investigating a complaint or alleged infringement of the GDPR relating to cross-border processing and preparing a draft decision on the matter. It then must coordinate, where possible, a consensus decision with other EU data protection authorities who are deemed to be 'concerned supervisory authorities'.

The DPC will be deemed a concerned supervisory authority where:

- a cross-border processing complaint has originally been lodged with the DPC but another Data Protection Authority (DPA) is the lead supervisory authority;
- where the processing in question substantially affects; or
- is likely to substantially affect, individuals in Ireland;
- or where the controller/processor is established in Ireland.

The lead supervisory authority must share its draft decision with *all* concerned supervisory authorities and consult with, and consider their views, in finalising the decision. Where this is not possible, the GDPR provides for a dispute-resolution mechanism to be triggered that will ultimately result in the members of the European Data Protection Board (EDPB) making a majority decision on the disputed issues in the draft decision.

In 2019, the DPC received 457 cross-border processing complaints through the OSS mechanism that were lodged by individuals with other EU data protection authorities.

Law Enforcement Complaints

The EU Directive known as the LED (EU 2016/680) was transposed into Irish law on 25 May 2018 with the enactment of the Data Protection Act 2018. In broad terms, LED applies where the organisation that is in control of the personal data is deemed a “competent authority” and the processing of personal data is carried out for the purposes of the prevention, investigation, detection or prosecution (PIDP) of criminal offences, or the execution of criminal penalties.

To distinguish, the LED would apply if a convicted offender complained to, for example, the Irish Prison Service that the data recorded about them was inaccurate. However, if the prison service received an access request from an employee about their own personal data, GDPR would apply.

In 2019, the DPC received 37 LED complaints, the majority relating to An Garda Síochána as the data controller, as well as the Irish Prison Service, the Revenue Commissioners, Veolia, Irish Rail and several local authorities.

Section 95 Reviews

Section 94 of the 2018 Act allows data controllers to restrict access to personal data on grounds such as the prevention of crime and to avoid prejudicing an investigation or prosecution. Where an individual is made aware that their rights have been restricted under the provisions of Section 94, they may request that the DPC independently review their case under Section 95.

In 2019, three reviews under Section 95 of the 2018 Act were conducted by the DPC in order to verify whether the restrictions imposed by the data controllers in question were lawful. In all four cases, the officers were satisfied the restrictions were lawful.

- One case concerned an individual who sought full access to their file. An Garda Síochána (AGS) had provided the individual with a copy of their data as recorded on PULSE but relied upon 94(3)(a) of the Act to restrict certain AGS communications concerning routine inter-agency operations as they were deemed to demonstrate operational methods and procedures employed by AGS. Upon review of the file, authorised officers of the DPC considered the processing was in compliance with *Part 5 of the Data Protection Act 2018 — Processing of Personal Data for Law Enforcement Purposes*. During the review, the data controller (AGS) clarified to authorised officers that it had no role or

input in relation to any data which may have been processed leading to the arrest of an Irish citizen at an airport outside of this jurisdiction. On foot of the section 95 review, the DPC conveyed this additional information to the individual.

- A section 95 review was conducted in connection with an individual who wanted a change made to records held about them by AGS. On inspection by the DPC, it was noted that the record related to unsolicited contact with a minor, resulting in an alert being raised. Officers from the DPC considered that the data recorded by AGS was in compliance with *Part 5 of the Data Protection Act 2018*.
- A section 95 review was conducted based on a complaint in which a couple alleged their data had been disclosed to their landlady by An Garda Síochána. An authorised officer from the DPC examined the file in question. Taking into account that An Garda Síochána had previously stated to the couple that no personal data was disclosed by them to their landlady, the DPC was satisfied based on the file viewed that all personal data inspected was in compliance with *Part 5 of the Data Protection Act 2018*.

Data-Breach Complaints

In 2019, the DPC handled 207 data-breach complaints from affected individuals, in comparison to the 48 data-breach complaints between 25 May 2018–December 31 2018. Trends indicate a significant rise in the number of breach complaints being made by individuals.

The majority of complaints related to unauthorised disclosures, predominantly:

- emails/letters to incorrect recipient;
- administrative processing errors;
- verbal disclosures;
- papers lost or stolen; and
- unauthorised access to personal data in the workplace.

Over the course of its engagement with individuals in 2019, the office has noted increased correspondence from individuals expressing dissatisfaction with the way businesses and organisations who control or process personal data have communicated with them, particularly regarding data breaches and the subsequent remedial actions the controller has taken. Greater adherence to Section 109(2) of the Data Protection Act 2018 would lead to earlier resolutions in many such instances and a reduction in the number of queries being brought forward to the DPC.

CASE STUDY 9 HSE Hospital/Healthcare Agency

In 2019, the DPC received a complaint about the disclosure of a patient's data via Facebook messenger by a hospital porter regarding her attendance at the Early Pregnancy Unit of a hospital. Upon examination of the complaint, the HSE clarified to the DPC that the hospital porter who disclosed the personal information of the patient was in fact employed by a healthcare agency contracted by the HSE. The DPC contacted the agency and sought an update in relation to its internal investigation, details of any remedial action as well as details of any disciplinary action taken against the employee in question. At the same time, the DPC advised the HSE that, as it contracts the company concerned to provide agency staff to work in the hospital, ultimately the HSE is the data controller for the personal data in this instance.

The complaint was subsequently withdrawn by the solicitor acting on behalf of the woman following a settlement being agreed between the affected party and the hospital/healthcare agency. Data controllers/data processors may be liable under Section 117 of the Data Protection Act 2018 to an individual for damages if they fail to observe the duty of care they owe in relation to personal data in their possession.

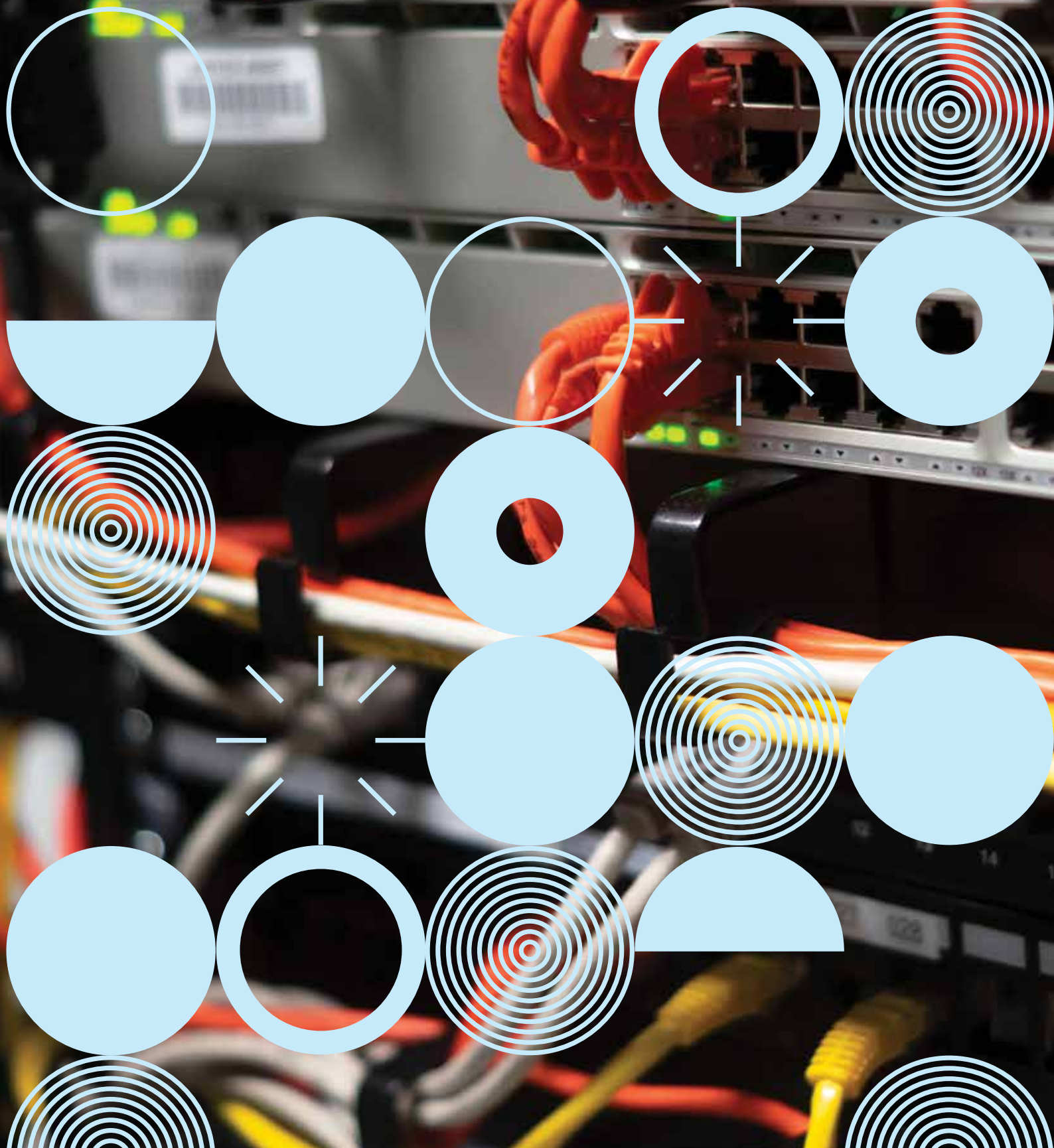
The DPC has no role whatsoever in dealing with compensation claims and no function in relation to the taking of any such proceedings under Section 117 of the 2018 Act or in the provision of any such legal advice.

What this case illustrates is that ongoing training is necessary for all staff in relation to their obligations under data

protection law and that controllers must do due diligence and satisfy themselves that any contractors/processors they engage are fully trained and prepared to comply with data protection laws.

5

Breaches



Data-Breach Notifications

The introduction of the GDPR brought with it mandatory data-breach notification obligations for all data controllers. The DPC undertakes a weekly analysis of breach notifications and processes a vast number of notifications received from areas within the public and private sector, including:

- the financial sector;
- the insurance sector;
- the telecommunications industry;
- the healthcare industry;
- the multi-national sector; and
- law enforcement.

Some of the trends and issues identified include:

- late notifications;
- difficulty in assessing risk ratings;
- failure to communicate the breach to individuals;
- repeat breach notifications; and
- inadequate reporting.

In 2019, the DPC received 6,257 data-breach notifications under article 33 of the GDPR. Of these 188 were classified as non-breaches due to the information involved not meeting the criteria to fall under the definition of personal data as set out in article 4.12 of the GDPR.

A total of 6,069 valid data breaches were received during 2019, representing an increase of 71% on the numbers reported in 2018. Unauthorised disclosures represent the highest classification of notified breaches across all sectors — 83% of all breaches.

Under GDPR a controller is obliged to notify the DPC of any personal data breach that has occurred, unless they are able to demonstrate that the personal data breach is 'unlikely to result in a risk to the rights and freedoms of natural persons'. This means that the default position for controllers is that all data breaches should be notified to the DPC, except for those where the controller has assessed the breach as being unlikely to present any risk to individuals and the controller can show why they reached this conclusion. In any event, for all breaches — even those that are not notified to the DPC on the basis that they have been assessed as being unlikely to result in a risk — controllers must record at least the basic details of the breach, the assessment thereof, its effects, and the steps taken in response, as required by Article 33(5) GDPR.

Businesses and organisations in control of personal data have an obligation to mitigate against all potential future breaches. The DPC has observed an increase in the number of repeat breaches of a similar nature by a large number of companies. This is most apparent in the financial sector, where the majority of breaches appear to be related to unauthorised disclosures. Data controllers can take simple steps to attempt to mitigate these risks such as running staff training and awareness programs; implementing stringent password policies and multifactor authentication for remote access; habitually update anti-virus and anti-malware software; ensuring that email and web filtering environments are correctly configured; and, ensuring that all computer devices are regularly updated with manufacturers' software and security patches.

Data breach notifications by category	Private	Public	Total
Disclosure (unauthorised)	3,249	1,939	5,188
Hacking	98	10	108
Malware	22	2	24
Phishing	138	23	161
Ransomware/denial of service	17	0	17
Software Development Vulnerability	13	0	13
Device lost or stolen (encrypted)	14	27	41
Device lost or stolen (unencrypted)	16	30	46
Paper lost or stolen	140	205	345
E-waste (personal data present on an obsolete device)	0	1	1
Inappropriate disposal of paper	20	24	44
System Misconfiguration	43	10	53
Unauthorised Access	67	64	131
Unintended online publication	44	41	85
Total	3,881	2,376	6,257

CASE STUDY 10

Loss of control of paper files

A public sector health service provider notified the DPC that a number of files containing patient medical information had been found in a storage cabinet on a hospital premises which was no longer occupied.

The records were discovered by a person who had gained illegally accessed a restricted premises and subsequently posted photographs of the cabinet containing the files on social media. The public sector organisation in question informed the DPC that, having become aware of the breach, a representative of the organisation was sent to locate and secure the files. The files were removed from the premises and secured.

This breach highlights the importance of having appropriate records management policies; including mechanisms for tracking files, appropriate secure storage facilities and full procedures for the retention or deletion of records.

The DPC issued a number of recommendations to the organisations to improve their personal data processing practices.

CASE STUDY 11

Ransomware Attack

An organisation operating in the leisure industry notified the DPC that it had been the victim of a ransomware attack which potentially encrypted/disclosed the personal data of up to 500 customers and staff stored on the organisation's server. The route of the infiltration was traced to a modem router that had been compromised (back up data was however stored securely via a cloud server).

Following examination of the incident, the DPC issued a number of recommendations to the organisation. The DPC recommended that the organisation conduct an analysis of its ICT infrastructure to establish if further malware was present, to review and implement appropriate measures to ensure there is an adequate level of security surrounding the processing of personal data, and to conduct employee training to encompass cyber security risks.

The DPC has received regular updates from the organisation and is satisfied that significant steps to improve and implement both organisational and technical measures concerning shortfalls in the security of their ICT infrastructure have been taken, including the development of a training plan for all staff in this area.

CASE STUDY 12

Disclosure of CCTV footage via social media

A commercial and residential property management company notified the DPC that an employee of a security company whose services they retained had used their personal mobile phone to record CCTV footage of two members of the public engaged in an intimate act, which had been captured by the management company's security cameras.

The video taken was subsequently shared via WhatsApp to a limited number of individuals. The business advised the DPC that they communicated to staff who may have received the footage that they must delete it and requested no further dissemination of the video.

Both the property management company and the security company were able to demonstrate that adequate policies and procedures did exist, however appropriate oversight and supervision to ensure compliance with these policies and procedures were lacking.

Following recommendations made by the DPC to the property management company, the company has subsequently engaged with its staff to deliver further data protection training with an emphasis on personal data breaches. In addition, further signage was displayed prohibiting the use of personal mobile devices within the confines of the CCTV control room.

6

Inquiries



Statutory Inquiries by the DPC

Under the Data Protection Act 2018, the DPC may conduct two different types of statutory inquiry under Section 110 in order to establish whether an infringement of the GDPR or the 2018 Act has occurred:

- a complaint-based inquiry; and
- an inquiry of the DPC's "own volition".

A statutory inquiry essentially consists of two distinct processes:

- the investigatory process, which is carried out by an investigator of the DPC; and
- the decision-making process.

The decision making process is carried out by a separate senior decision-maker in the DPC who has had no role in the investigatory process, usually the Commissioner for Data Protection.

The objective of any inquiry is to:

- establish the facts as they apply to the matters under investigation;
- apply the facts as found to the provisions of the GDPR and/or 2018 Act as applicable in order to analyse whether an infringement of the GDPR and/or 2018 Act has been identified;
- make a formal decision of the DPC in relation to whether or not there is an infringement; and
- where an infringement has been identified, make a formal decision on whether or not to exercise a corrective power, and if so, which corrective power.⁴

During the investigatory process of an inquiry, authorised officers may be appointed by the DPC and they may exercise a range of investigatory powers under the 2018 Act in the context of an inquiry. In addition to the general power to issue an information notice compelling the provision of specified information to the DPC, an authorised officer has a broad range of investigatory powers at his/her disposal enabling them to gather relevant information, documents and materials⁵. These include powers of entry, search and inspection of premises, equipment, documents and information, the removal and retention of documents and records, and requiring information and assistance to be provided to them in relation to access to documents and records and equipment. There is also a power to apply to the District Court for a warrant to enter a premises in order to exercise the authorised officer powers.

On 31 December 2019, the DPC had 70 statutory inquiries on hand, including 21 cross-border inquiries.

⁴ Corrective powers include imposing an administrative fine (not applicable for infringements of the LED), issuing a warning, a reprimand, a temporary or definitive ban on processing or a suspension of international data transfers or a direction to bring processing into compliance, amongst others.

⁵ In the context of an existing inquiry, the DPC may also launch a statutory "investigation" under Section 137. A Section 137 investigation carries specific additional investigatory powers, such as the power of the authorised officer conducting it to hold an oral hearing. To date the DPC has not commenced any Section 137 investigations.

Multinational Technology Company Statutory Inquiries commenced since 25 May 2018

Company	Inquiry type	Issue being examined
Facebook Ireland Limited	Complaint-based inquiry	<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 inquiry	<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 inquiry	<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 inquiry	<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 inquiry	<i>Facebook September 2018 token breach.</i> Examining Facebook's compliance with the GDPR's breach notification obligations.
Facebook Inc.	Own-volition inquiry	<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	Own-volition inquiry	<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 inquiry	<i>Facebook passwords stored in plain text format in its internal servers.</i> Examining Facebook's compliance with its obligations under the relevant provisions of the GDPR.
WhatsApp Ireland Limited	Complaint-based inquiry	<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 inquiry	<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.

Green indicates inquiries opened between 25 May 2018 – 31 December 2018.
White indicates inquiries opened in 2019.

Company	Inquiry type	Issue being examined
Instagram (Facebook Ireland Limited)	Complaint based inquiry	<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
Apple Distribution International	Complaint-based inquiry	<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 inquiry	<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 inquiry	<i>Right of Access.</i> Examining whether Apple has complied with the relevant provisions of the GDPR in relation to an access request.
Twitter International Company	Complaint-based inquiry	Right of Access. Examining whether Twitter has discharged its obligations in respect of the right of access to links accessed on Twitter.
Twitter International Company	Own-volition inquiry	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 inquiry	Commenced in response to a breach notification. Examining an issue relating to Twitter's compliance with Article 33 of the GDPR.
LinkedIn Ireland Unlimited Company	Complaint-based inquiry	<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.
Quantcast International Limited	Own-volition inquiry	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.
Google Ireland Limited	Own-volition inquiry	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.
Verizon Media/Oath	Own-volition inquiry	<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.

Ongoing Cross-Border Inquiries

Apple Distribution International (transparency obligations)

This complaint-based inquiry arises from a complaint initially lodged by the complainant in Germany but then transferred to the DPC, as the lead supervisory authority for the controller in question, as the main establishment of Apple is in Ireland. The complainant alleges that the controller is contravening Articles 12 and 13 of the GDPR by failing to provide certain required information to individuals, such as the identity and contact details of the controller's representative and data protection officer, the legal basis for processing and the storage period of any personal data collected. The inquiry is focused on an examination of the controller's compliance with its transparency obligations, looking at the information which is provided to users by the controller on its website. This includes assessing the manner in which a layered approach to provision of information can/should be used, as well as the timing of provision of information to individuals.

Apple Distribution International (access request issues)

This complaint-based inquiry relates to an access request made by the complainant for customer service records from Apple where the complainant was dissatisfied with Apple's response to his access request. In this case, the controller's position is that the request by the complainant was 'manifestly excessive'. The inquiry involves an examination of the extent to which a data controller may refuse to act on an access request, in circumstances where that controller believes that the request is "manifestly unfounded or excessive", as referred to in Article 12 GDPR.

Apple Distribution International (legal basis for processing in context of targeted advertising to users)

This complaint-based inquiry is examining whether the controller 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. The complaint in question was lodged by a French digital advocacy organisation, La Quadrature du Net, through Article 80 of the GDPR whereby a data subject can mandate a not-for-profit body to lodge a complaint and act on his/her behalf. The issues under investigation include whether or not the processing of personal data, in this context, is supported by a legal basis, as required by Article 6 of the GDPR, and, if so, which one(s). This entails consideration of the conditionality and limitations associated with reliance on certain legal bases, such as consent and the legitimate interests of the data controller or a third party. Co-operation with the CNIL (the French supervisory authority with which the complaint giving rise to this inquiry was originally filed) is ongoing.

Facebook Ireland Limited (legal basis for processing and transparency in relation to Terms of Service and Data Policy)

This complaint-based inquiry arose from a complaint received from the Austrian privacy advocacy organisation NOYB (None of Your Business) which focused on Facebook's Terms of Service and Data Policy for its users. The inquiry is examining whether Facebook has complied with the obligation to have a legal basis to process personal data of individuals using the Facebook platform. The inquiry also includes an examination of whether Facebook provided the data subject with information on its legal basis for processing in connection with its Terms of Service, and addresses the complainant's contention that processing in connection with Facebook's Terms of Service was conducted on the basis of the data subject's consent but that that consent was not valid having regard to the nature of the consent which is required under the GDPR.

Facebook Ireland Limited (legal basis for processing in context of targeted advertising to users)

This complaint-based inquiry is examining whether Facebook has complied with its obligations in respect of the requirement to have a legal basis for processing personal data in the context of behavioural analysis and targeted advertising of Facebook users on its platform. The complaint in question was lodged by a French digital advocacy organisation, La Quadrature du Net. Amongst other things, this inquiry involves a detailed examination of the processing operations underpinning the analysis of users' behaviour/ activities (including profiling) on the Facebook platform and how that relates to the delivery of targeted advertisements to the user. Co-operation with the CNIL (the French supervisory authority with which the complaint giving rise to this inquiry was originally filed) is ongoing.

Facebook Ireland Limited (security incident concerning storage in plain text of user passwords)

This is an inquiry examining whether Facebook complied with its obligations under the GDPR in relation to a security incident which occurred in early 2019. In this case, Facebook confirmed to the DPC that user passwords had been inadvertently stored in plaintext on its internal systems. This inquiry is examining whether Facebook's conduct in relation to this incident amounted to an infringement of any provision(s) of the GDPR, and in particular whether Facebook, in storing user passwords in plaintext format, complied with its obligations in relation to data security. The inquiry is also examining whether the storage of user passwords in this manner amounted to a personal data breach for the purposes of Article 33 of the GDPR.

Facebook Ireland Limited (access request for certain technical information)

This a complaint-based inquiry was initiated on foot of a complaint made to the DPC by a data subject, regarding Facebook's handling of a data subject access request and data portability request made by him. The inquiry is examining whether Facebook has complied with its obligations in relation to the complainant's exercise of the right of access to his personal data and the right to data portability in respect of personal data held in a certain technical database by Facebook. The complainant had requested, amongst other things, to be provided with a copy of specific personal data relating to him, including personal data held, indexed alongside or related to his User ID which was held in raw format; and a copy of personal data that had been provided by or observed about him in a machine readable format. This inquiry is examining the extent of the data subject rights to access and portability under the GDPR, having regard to Article 12 of the GDPR, including the extent to which a data controller may refuse to act on a data subject request in circumstances where that controller believes that the request is "manifestly unfounded or excessive", as referred to in Article 12 GDPR.

Google Ireland Limited (legal basis for, and transparency of, Google's real time bidding and Google Authorised Buyers system)

This is an own-volition inquiry, which was commenced, following the receipt by the DPC of certain submissions made to it by Dr Johnny Ryan of Brave, is examining the processing of personal data by Google in the context of targeted advertising. More specifically, the inquiry is examining the processing of personal data in the context of the 'Real-Time Bidding' (RTB) process facilitated by Google's proprietary Authorised Buyers mechanism, which facilitates targeted advertising. In terms of its scope, the inquiry is examining, amongst other things, whether Google has a legal basis for processing personal data, which may include special category data, via the Google Authorised Buyers mechanism. The inquiry is also examining how Google fulfils its transparency obligations in relation to the processing of such personal data, as well as its obligations concerning the retention of such personal data in the context of the Google Authorized Buyers Ad Exchange.

Instagram (Facebook Ireland Limited) (legal basis for processing and transparency in relation to Terms of Use and Data Policy)

This complaint-based inquiry arising from a complaint received from the Austrian privacy advocacy organisation NOYB (None of Your Business) which focused on Instagram's Terms of Use and Data Policy for its users. The inquiry is examining whether Instagram has complied with the obligation to have a legal basis to process personal data of individuals using the Instagram platform. The inquiry includes an examination of whether Instagram provided the data subject with information on Instagram's legal basis for processing in connection with its Terms

of Use. It also addresses the complainant's contention that processing in accordance with WhatsApp's Terms of Service was conducted on the basis of the data subject's consent but that that consent was not valid having regard to the nature of the consent which is required under the GDPR.

LinkedIn Ireland Unlimited Company (legal basis for processing in context of targeted advertising to users)

This complaint-based inquiry into LinkedIn is focused on examining whether LinkedIn has complied with its GDPR obligations, in particular in respect of the requirement to have a legal basis for processing personal data, in the context of behavioural analysis and targeted advertising on its platform. The complaint in question was lodged by a French digital advocacy organisation, La Quadrature du Net, through Article 80 of the GDPR whereby a data subject can mandate a not-for-profit body to lodge a complaint and act on his/her behalf. Issues that the DPC is specifically examining, and which formed part of the complaint, include the issue of whether consent and another legal basis can be relied upon jointly for processing. Amongst other things, this inquiry involves a detailed examination the technological framework underpinning the analysis of users' behaviour/ activities (including profiling) on the LinkedIn platform and how that relates to the delivery of targeted advertisements to the user. Co-operation with the CNIL (the French supervisory authority with which the complaint giving rise to this inquiry was originally filed) is ongoing.

Quantcast International Limited (legal basis for processing and transparency in profiling and targeted advertising)

This own-volition inquiry was commenced by the DPC following a submission which was made to the DPC by Privacy International, a privacy advocacy organisation, concerning Quantcast which provides services to entities operating in the adtech sector. In particular, the DPC is examining whether Quantcast has discharged its obligations in connection with the processing and aggregating of personal data which it conducts for the purposes of profiling and utilising the profiles generated for targeted advertising. The inquiry is examining how, and to what extent, Quantcast fulfils its obligation to be transparent to individuals in relation to what it does with personal data (including sources of collection, combining and making the data available to its customers) as well as Quantcast's personal data retention practices. The inquiry will also examine the lawful basis pursuant to which processing occurs.

Twitter International Company (right of access and right to data portability)

This complaint-based inquiry arises from a complaint by a Twitter user in relation to an access and portability request which was made to Twitter whereby the user sought certain technical information (related to user interaction with web links generated by Twitter). This

request was refused by Twitter. The inquiry examines whether Twitter has discharged its obligations in respect of the right of access and the right to data portability to personal data having regard to Article 12 of the GDPR and the extent to which a data controller may refuse to act on a data subject request in circumstances where that controller believes that the request is “manifestly unfounded or excessive”, as referred to in Article 12 GDPR.

WhatsApp Ireland Limited (legal basis for processing and transparency in relation to Terms of Service and Privacy Policy)

This complaint-based inquiry arose from a complaint received from the Austrian privacy advocacy organisation NOYB (None of Your Business) which focused on WhatsApp's Terms of Service and Privacy Policy for its users. The inquiry is examining whether WhatsApp has complied with the obligation to have a legal basis to process personal data of individuals using the WhatsApp platform. The inquiry includes an examination of whether WhatsApp provided the data subject with information on WhatsApp's legal basis for processing in connection with its Terms of Service. The inquiry also addresses the complainant's contention that processing in accordance with WhatsApp's Terms of Service was conducted on the basis of the data subject's consent but that that consent was not valid having regard to the nature of the consent which is required under the GDPR.

Facebook Ireland Limited (breach notification obligations — “token” breach)

This own-volition inquiry was commenced following a breach notification made to the DPC by Facebook concerning an incident where an external actor obtained Facebook user tokens. (User tokens enable the authentication of the related Facebook user account i.e. they keep the user logged into Facebook so that they do not need to re-enter their password every time they use the Facebook app). Following the incident, Facebook reset millions of user tokens for Facebook accounts. The inquiry is examining Facebook's compliance with the breach notification obligations in Article 33 GDPR and amongst other things, involves an assessment of the information provided by Facebook to the DPC in relation to the incident, the timing of same and the internal documentation of the data breach by Facebook.

Facebook Ireland Limited (technical and organisational measures — “token” breach)

This own-volition inquiry was commenced following the same breach notification made to the DPC by Facebook as in the preceding inquiry, where an external actor obtained Facebook user tokens. (User tokens enable the authentication of the related Facebook user account i.e. they keep the user logged into Facebook so that they do not need to re-enter their password every time they use the Facebook app). As referred to above, following the incident, Facebook reset millions of user tokens for Facebook accounts. This inquiry is examining Facebook's compliance with its obligations, pursuant to articles 32, 24,

and 5 of the GDPR, to implement appropriate technical and organisational measures and amongst other things, involves an assessment of the information provided by Facebook to the DPC in relation to the incident and an assessment the policies and procedures Facebook had in place at the time the incident occurred.

Facebook, Inc. (technical and organisational measures — “token” breach)

This own-volition inquiry was commenced following the same breach notification made to the DPC by Facebook as in the two preceding inquiries, where an external actor obtained Facebook user tokens. (User tokens enable the authentication of the related Facebook user account i.e. they keep the user logged into Facebook so that they do not need to re-enter their password every time they use the Facebook app). As referred to above, following the incident, Facebook reset millions of user tokens for Facebook accounts. This inquiry is examining Facebook Inc.'s compliance with its obligations, pursuant to articles 32 and 5 of the GDPR, to implement appropriate technical and organisational measures and amongst other things involves an assessment of the information provided by Facebook Inc. to the DPC in relation to the incident and an assessment the policies and procedures Facebook Inc. had in place at the time the incident occurred.

Facebook Ireland Limited (multiple breaches)

This own-volition inquiry was commenced following a number of breach notifications made to the DPC by Facebook Ireland Limited concerning unauthorised disclosure of personal data. The inquiry is examining Facebook's compliance with its obligations, pursuant to articles 32, 24, and 5 of the GDPR, to implement appropriate technical and organisational measures and amongst other things, involves an assessment of the information provided by Facebook to the DPC in relation to the incidents and an assessment the policies and procedures Facebook had in place at the time the incidents occurred.

Twitter International Company (multiple breaches)

This own-volition inquiry was commenced following a number of breach notifications made to the DPC by Twitter concerning unauthorised disclosure of personal data. The inquiry is examining Twitter's compliance with its obligation, pursuant to articles 32, 24, and 5 of the GDPR, to implement appropriate technical and organisational measures and amongst other things, involves an assessment of the information provided by Twitter to the DPC in relation to the incidents and an assessment the policies and procedures Twitter had in place at the time the incidents occurred.

Oath (EMEA) Ltd/Verizon Media (transparency)

This own-volition inquiry was opened into Verizon Media/Oath (EMEA) Limited in respect of the company's compliance with its transparency obligations under Articles 12, 13 and 14 of the GDPR. This inquiry was commenced under section 110(1) of the Data Protection Act 2018

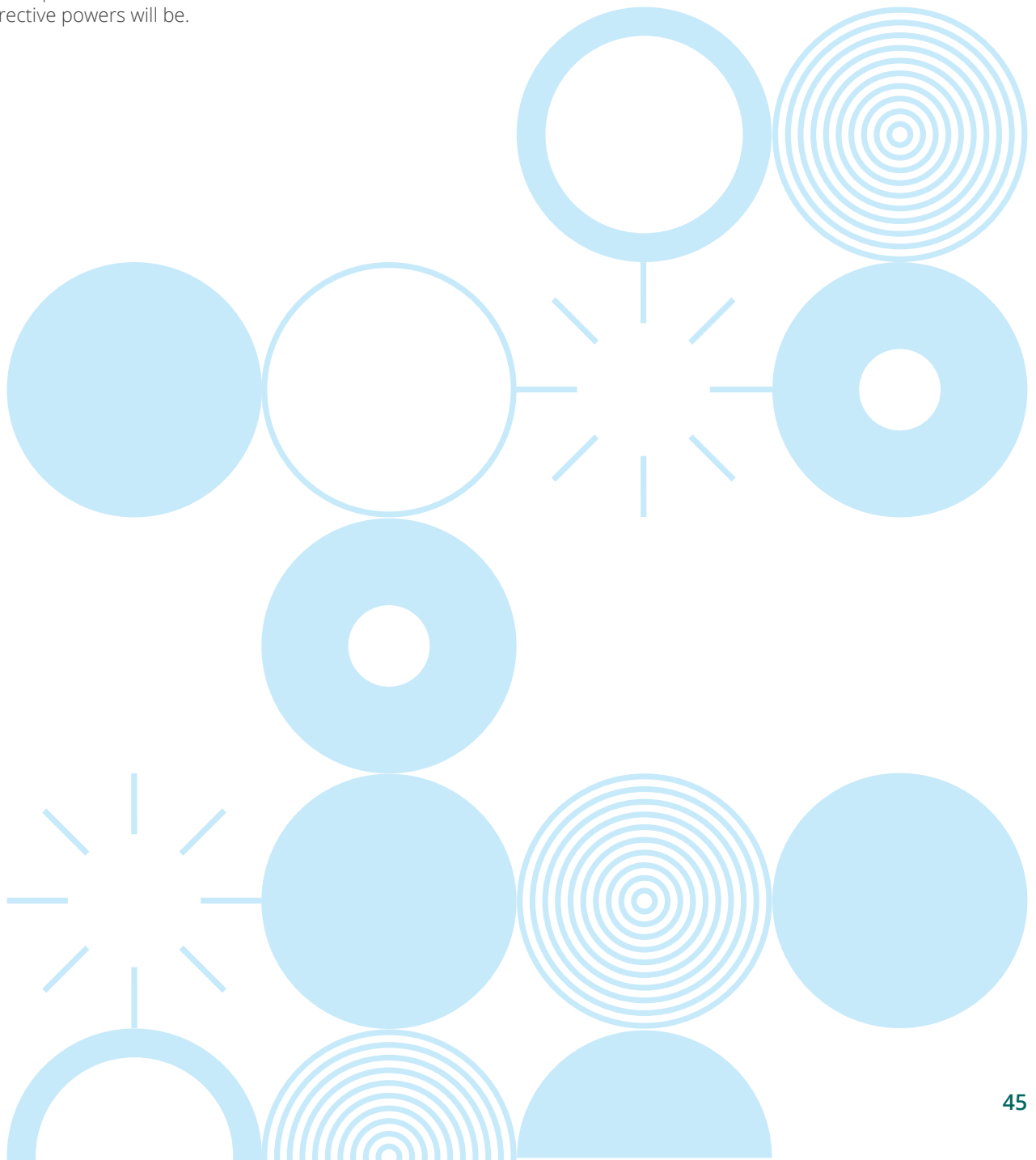
following assessment of a number of complaints regarding Oath products and services, including some from individuals in other EU member states. The inquiry was in the information-gathering phase as of the end of 2019.

WhatsApp Ireland Limited (transparency)

This own-volition inquiry was commenced following a number of complaints made by data subjects throughout Europe about the transparency of WhatsApp Ireland’s data sharing with the Facebook family of companies and transparency surrounding its use of non-user data, focusing on transparency obligations under Articles 12, 13 and 14 of the GDPR. The investigative stage of the process being complete, the final inquiry report has been passed to the Commissioner, who is the decision-maker under Section 111 of the Data Protection Act 2018. The Commissioner will prepare a draft decision which will be circulated to other European DPAs for comment pursuant to Article 60 GDPR. A final decision will then be made by on whether the GDPR has or is being infringed, whether any corrective powers will be exercised, and if so, what those corrective powers will be.

Twitter International Company (breach notification)

This own-volition inquiry was commenced following a breach notification made to the DPC by Twitter concerning a bug in Twitter’s Android app, where users who changed the email address associated with their account had all of their protected tweets made public. The focus is on the obligation to make breach notifications in a timely manner under Article 33(1) of the GDPR, and the obligation to document data breaches under Article 33(5) of the GDPR. The investigative stage of the process being complete, the final inquiry report has been passed to the Commissioner, who is the decision-maker under Section 111 of the Data Protection Act 2018. The Commissioner will prepare a draft decision which will be circulated to other European DPAs for comment pursuant to Article 60 GDPR. A final decision will then be made on whether the GDPR has or is being infringed, whether any corrective powers will be exercised, and if so, what those corrective powers will be.



Ongoing National Inquiries

Domestic Statutory Inquiries commenced since 25 May 2018

Green indicates inquiries opened between 25 May 2018 – 31 December 2018.
White indicates inquiries opened in 2019.

Organisation	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.
Bank of Ireland	Own Volition	Commenced in response to the large number of breaches notified to the DPC during the period since 25 May 2018.
Catholic Church	Own Volition	Multiple complaints re right to rectification & right to be forgotten
DEASP	Own Volition	Examining the position of the Data Protection Officer under Article 38 of the GDPR.
SUSI	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 it 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.
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.
Slane Credit Union	Own Volition	Commenced in response to a breach notified to the DPC in relation to an unauthorised disclosure.
HSE Mid Leinster (Tullamore Labs)	Own Volition	Commenced in response to a breach notified to the DPC.
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.
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.

University of Limerick

This inquiry relates to a notified breach about an incident of phishing which the controller became aware of in November 2018, along with three previous phishing breaches notified in February, April and May 2018. The inquiry commenced in July 2019. A further phishing breach was notified in August 2019.

379 individuals were impacted in the November 2018 breach.

An on-site inspection will be carried out in early 2020.

University College Dublin

This inquiry relates to seven breach notifications received between September 2018 and January 2019.

The university reported that email accounts across multiple university schools were compromised and were detected to be sending spam. Some of the breaches related to users furnishing their credentials on external websites and, in other cases, the controller was unable to identify how its systems were compromised. The account credentials had been posted publicly online for some users. Other credentials were identified in "haveibeenpwnd.com".

The inquiry commenced in July 2019. A site inspection has been carried out and a Draft Inquiry Report is being prepared.

Maynooth University

This inquiry relates to an instance of hacking of a university's employee email account. The email account of an employee at Maynooth University was hacked and forwarding rules were set. Subsequent correspondence between that employee and another staff member was intercepted and bogus bank account details were substituted, causing a money transfer of a lump sum of €28,823.40 to be diverted.

Initial analysis by the university indicated attempted phishing, but there was no indication of any successful phishing. The employee's personal computer had malware on it since 2017. The particular malware was a Trojan often used as a launchpad to download malicious software. The university found no indication of the method used to place that malware on the personal computer.

The attacked email account was only one of six accounts potentially accessed. However, the university has not found any evidence of exploitation of the other five accounts. For all six accounts there is a risk that there were substantial amounts of personal data within the emails that may have been disclosed/accessed.

This inquiry commenced in November 2019 and is ongoing.

Bank of Ireland

This inquiry relates to 22 breach notifications from Bank of Ireland, in which the bank was sending inaccurate data to the Central Credit Register, with a corresponding risk

that the credit rating of certain bank customers had inaccurate information recorded.

The inquiry commenced in November 2019 and is ongoing.

Irish Credit Bureau

This inquiry relates to a breach notification that the DPC received from the Irish Credit Bureau (ICB) in relation to a data integrity issue. A change to the ICB system inadvertently allowed incorrect updates to be applied to the loan account records of financial institutes' customers.

The issue impacted on the credit ratings of 15,238 individuals. 118 individuals had requested their credit report directly from the ICB while the data was incorrect.

The inquiry commenced in July 2019. The next step of the inquiry is to furnish a Draft Inquiry Report to the ICB.

Slane Credit Union

This inquiry relates to a breach notification received from Slane Credit Union, where the credit union publically disclosed personal data of 78 account holders via general searches on the internet. A plug-in on the credit union's website had indexed the private content of the credit union pages and made it available as public content, which could subsequently be accessed using generic searches about Slane village. Oversight of the website had been outsourced to a separate company, who acted as a data processor.

The inquiry commenced in July 2019 and an on-site inspection has taken place where the data controller and processor were questioned about data protection management. The next step is to issue a Draft Inquiry Report.

HSE (South)

This inquiry relates to the discovery of hospital records by a member of the public. Hospital documents containing personal data (name, date of birth, clinical details, and treatment) of 56 patients were found by a member of the public at a public recycling facility in Cork. Previously, there had been seven similar breaches reported to the DPC for the same HSE Area.

This inquiry commenced in October 2019. A Draft Inquiry Report has been issued to the HSE.

HSE (Our Lady of Lourdes Hospital)

This inquiry relates to the discovery of hospital records by a member of the public. The inquiry was commenced in November 2019 as a result of hospital ward handover documents relating to 15 patients being discovered by a member of the public in her front garden. A very similar incident had occurred in March 2019 when handover notes on eight patients were discovered on the public road outside the same hospital.

A Draft Inquiry Report is in preparation.

HSE Mid-Leinster (Tullamore)

This inquiry relates to a breach notification about ransomware activated on the computers within the HSE Laboratories in Tullamore. The data controller understood that ICT security measures had been delegated to a data processor. The inquiry commenced in October 2019 and is ongoing.

Tusla (November 2018)

This inquiry relates to 71 personal data disclosure breaches notified by *Tusla — The Child and Family Agency* to the DPC. The inquiry began in November 2018.

The subject matter of the breaches included inappropriate system access, disclosure by email and post and security of personal data.

The DPC conducted site inspections at Tusla headquarters and at regional offices in Dublin Central, Naas, Swords, Waterford, Galway and Cork. In the course of the inspections, a number of other data protection issues came to light which fell outside the original scope of the Inquiry. However, as these issues have relevance with regard to the protection of personal data, they will be highlighted in the Draft Inquiry Report.

The DPC is currently preparing the Draft Inquiry Report.

Tusla (October 2019)

This inquiry relates to three breach notifications received between February and May 2019 relating to unauthorised disclosure of personal data.

In one breach, Tusla accidentally disclosed the contact and location data of a mother and child victim to an alleged abuser.

In the next breach, Tusla accidentally disclosed contact, location and school details of foster parents and children to a grandparent. As a result, that grandparent made contact with the foster parent about the children.

In the third breach, Tusla accidentally disclosed the address of children in foster care to their imprisoned father, who used it to correspond with his children.

The inquiry commenced in October 2019. A Draft Inquiry Report has issued to Tusla.

Tusla (November 2019)

This inquiry relates to a breach notification received from Tusla in November 2019 regarding an unauthorised disclosure of sensitive personal data. The disclosure was made to an individual against whom an allegation of abuse had been made.

The disclosed data was subsequently posted on social media.

This inquiry commenced in December 2019.

Department of Employment Affairs and Social Protection (DEASP) DPO

This inquiry relates to potential infringements of Article 38 of the GDPR in relation to the Department's interactions with its Data Protection Officer in the Department of Employment Affairs and Social Protection. The inquiry began in December 2018. A Draft Inquiry Report was issued to the Department in May 2019 and the controller made submissions on it. These have been analysed by the DPC and the Final Inquiry Report is in preparation.

Catholic Church

This inquiry relates to the lawful basis for processing the personal data of individuals who no longer want to have their personal data so processed. The DPC received a number of complaints from individuals who were members of the Catholic Church and many of whom no longer wished to remain as members. In the absence of a way to defect formally from the Catholic Church, the individuals expressed dissatisfaction with the ongoing processing of their personal data by the Catholic Church, in particular the retention of their personal data on sacramental registers. As a consequence, each individual had requested the erasure of their church records, including those contained in baptism, confirmation and marriage registers. In all instances the request for erasure had been refused by the relevant parish offices.

Having considered the issue at a preliminary level, the DPC has opened an own-volition inquiry pursuant to section 110(1) of the Data Protection Act 2018. This inquiry is directed to the Archdiocese of Dublin and will examine whether there is a lawful basis for the processing of the personal data of individuals who no longer want to have their personal data so processed.

An Garda Síochána

This inquiry relates to the process and procedures governing disclosure requests to external third party data controllers by An Garda Síochána (AGS). The inquiry commenced in April 2019. Within the context of the inquiry, pursuant to section 136 of the Data Protection Act 2018, 8 data protection audits were conducted of AGS and a selection of organisations processing disclosure requests received from AGS.

The next step of the inquiry is to furnish a Draft Inquiry Report to AGS.

Irish Prison Service

The DPC opened an own-volition inquiry into the Irish Prison Service, specifically into the governance procedures in place regarding the processing of personal data by the work of the Operational Support Group. This inquiry is in its initial stages.

Student Universal Support Ireland (SUSI)

This inquiry relates to a breach notification received from the City of Dublin Education and Training Board (CDET) in relation to its Student Universal Support Ireland (SUSI)

website. The website had a breach, where malicious code (a web-shell) was detected by the SUSI IT team on 16 October 2018. The inquiry is examining the technical and organisational measures in place at the time of the breach, and how SUSI has discharged its obligations as a data controller following the breach. The inquiry commenced in July 2019 and is ongoing.

Surveillance by the State Sector for Law Enforcement Purposes

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. While the use of such technologies for surveillance purposes by the state for law-enforcement functions has become more widespread and while there may be a perception by many that surveillance has become the norm, this perception does not diminish the obligations placed on organisations processing personal data through these means. Furthermore, while the usefulness of such technology for surveillance purposes may be obvious, i.e. the detection of specific security relevant incidents, surveillance systems operating in public places can impact on the privacy of individuals. As such it is essential that organisations in control of such systems can demonstrate that their systems are operating in compliance with data protection legislation.

The type of CCTV camera 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 so they may pose higher risks to individuals' privacy. Furthermore, the deployment of ANPR cameras is becoming more common place in the State Sector but the absence of data protection policies governing the use of such technology in the State Sector is notable.

These concerns prompted the DPC to commence a number of own-volition inquiries under the Data Protection Act 2018 into 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, which is becoming an increasingly prevalent part of CCTV systems. There are several other aspects to these ongoing own-volition inquiries such as an examination of the use of CCTV cameras to monitor certain local-authority housing estates and the use of covert cameras to detect offenders in the act of littering and unlawful waste disposal. The inquiries are also examining the legal basis underpinning the use of these surveillance technologies for law-enforcement purposes.

These own-volition inquiries are being conducted under Section 110 and Section 123 of the Data Protection Act 2018 and they have been split into a number of modules. The first module focuses on the 31 local authorities in Ireland, and the second module focusses on An Garda Síochána. Further modules are likely to be added as the inquiries progress. The first and second modules com-

menced using the data protection audit power provided for in Section 136 of the Data Protection Act 2018.

In the first phase of the audits, the DPC issued a detailed questionnaire to all 31 local authorities and to An Garda Síochána to elicit information in relation to their respective usage of CCTV, body-worn cameras, ANPR-enabled systems, drones and other technologies for surveillance purposes. The second phase, i.e. the information gathering phase, began in September 2018 with a series of on-site inspections.

To date, the DPC has conducted inspections in seven separate local authorities. The local authorities inspected were 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 1,000 CCTV cameras in operation for surveillance purposes. *Note: The inquiries do not apply to security cameras such as those deployed for normal security purposes.* Each of the local authorities inspected had its own unique approach to how it conducted surveillance on citizens. As part of the inquiry process, the DPC sought evidence of robust data protection policies as well as evidence of active oversight and meaningful governance.

Another key aspect of these inquiries involves auditing the deployment of community-based CCTV systems by examining whether Section 38(3)(c) of the Garda Síochána Act 2005 (which provides a legislative basis for such schemes under certain conditions) is being fully complied with. Community-based CCTV schemes that have been set up at local level require that the local authority be a data controller and that prior authorisation of the Garda Commissioner is required. In particular, the inquiries are examining whether or not the Garda Commissioner has approved all such schemes in operation at present (to date the Garda Commissioner has authorised Community-based CCTV schemes in approximately seventy cities, towns and villages across the State). The inquiries are also examining how data controller obligations are being met by the local authorities as required under that Act.

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). Currently there are approximately 38 separate schemes that operate under this legislation that are solely under the control of An Garda Síochána. The inquiry conducted involved inspections at Garda Stations in Tullamore, Henry Street Limerick, Pearse Street Dublin, Duleek and Ashbourne Co. Meath.

Following the submission of the final inquiry report to the Commissioner for Data Protection, the Commissioner made 13 findings in respect of infringements of the Data Protection Act, 2018. These infringements relate to a number of matters such as governance issues (including record-keeping of downloads, retention periods, training, auditing of access logs); transparency in relation

to informing the general public by signage and other means; the absence of data processor contracts; and the deployment of ANPR cameras on one Garda scheme in the absence of the implementation of appropriate data protection policies by An Garda Síochána and its failure to carry out a data protection impact assessment before rolling out the scheme. *Note: As the matters under examination related to the law enforcement provisions of the Data Protection Act 2018 only, infringements of the GDPR did not arise in these instances.*

The Commissioner decided to exercise three corrective powers in accordance with Section 127 of the Data Protection Act, 2018. In summary, a reprimand was issued to An Garda Síochána in circumstances where the processing was not in compliance with the 2018 Act and in such instances the Commissioner ordered the processing to be brought into compliance. Furthermore a temporary ban was imposed on processing in one region where such processing involves the operation of ANPR cameras until such time as their necessity and justification can be demonstrated. An Garda Síochána switched off these ANPR cameras as ordered by the Commissioner within seven days.

Cookies Sweep 2019 (Carried out under the GDPR and ePrivacy Regulations)

In August 2019, the DPC commenced an examination of the use of cookies and similar technologies on a selection of websites across a range of sectors, including media and publishing, the retail sector, restaurants and food ordering services, insurance, sport and leisure and the public sector.

The purpose of the sweep survey was to request information to allow us to examine the deployment of such technologies and to establish how, and whether, organisations are complying with the law. In particular, we wanted to examine how controllers obtain the consent of users for the use of cookies and other tracking technologies.

The standard of consent that controllers must obtain from users or subscribers for the use of cookies must now be read in light of the GDPR standard of consent, i.e. it must be obtained by means of a clear, affirmative act and be freely given, specific, informed and unambiguous.

There was a good level of cooperation with the sweep and most organisations were keen to demonstrate compliance. In some cases they signalled their awareness that they may not currently be compliant with S.I. No. 336/2011 — the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 ('the ePrivacy Regulations') and they wished to obtain guidance from the DPC on how to amend their practices, if required.

The quality of information provided to users in relation to cookies varied widely. Some organisations provided detailed and layered information about the technologies in use, and others provided little detail about the use of cookies, or about how to reject them.

We also established that many organisations are setting a wide range of cookies as soon as a user lands on their

website, without any engagement by the user with a consent management platform or cookie banner. These included third-party cookies from social media companies, payment providers and advertisers.

Many organisations categorised the cookies deployed on their websites as having a 'necessary' or 'strictly necessary' function, or a 'performance', 'functional' or 'analytics' function.

However, some cookies defined by controllers in their responses as 'strictly necessary' appear not to meet either of the two consent exemption criteria set down in the ePrivacy Regulations.

There was some level of awareness, particularly among larger organisations, of recent or pending rulings by the Court of Justice of the European Union (CJEU) in the ePrivacy area, which may impact on their practices. Some are reassessing issues of joint controllership that may arise in respect of the use of third-party plugins and social 'like' buttons in light of the *Fashion ID* judgment of 29 July 2019.

On 1 October, shortly after the DPC commenced this sweep, another significant judgment from the CJEU in the *Planet49* case clarified that consent for the placement of cookies is not valid if it is obtained by way of pre-checked boxes which users must deselect to refuse their consent.

The use of pre-checked boxes and sliders set by default to the 'on' position was a feature on a number of the websites we examined. In addition, many organisations relied on implied consent to set cookies, or they directed users to their browser settings to control cookies.

There were also examples of pre-checked boxes which opted users in to analytics and marketing cookies by default, but with the organisation failing to honour any choice expressed by the user if they unchecked the boxes. A lack of clarity on how users could withdraw their consent to cookies was also a feature on some sites.

During 2020, the DPC will produce updated guidance on cookies and other technologies which will take account of the judgments in *Planet49* and *Fashion ID*. This guidance will underpin our future enforcement strategy and activity.

Given the pervasive nature and scope of online tracking, and the inextricable links between such tracking and cookie technologies and adtech, we will place a strong focus on compliance in this area.

Other Investigations (Under the Data Protection Acts 1988 and 2003)

Tusla Child and Family Agency Investigation

In November, the DPC concluded an investigation that had commenced in March 2017 (under the Data Protection Acts 1988–2003 which were applicable at the time) into the governance of personal data within the Child and Family Agency, Tusla.

The investigatory phase, which included physical inspections by our Authorised Officers at Tusla locations around the country, had been completed in December 2017.

The DPC continued to engage with Tusla throughout 2018 and 2019 in relation to a number of our findings, including in relation to issues related to the co-location of Tusla offices with facilities also occupied by the Health Service Executive (HSE).

The agency confirmed that a number of organisational and technical measures have been put in place since the DPC's site inspections in late 2017. Tusla's ICT unit is also advancing what the agency describes as "a significant work programme" which will see the establishment of an ICT environment wholly managed and controlled by Tusla.

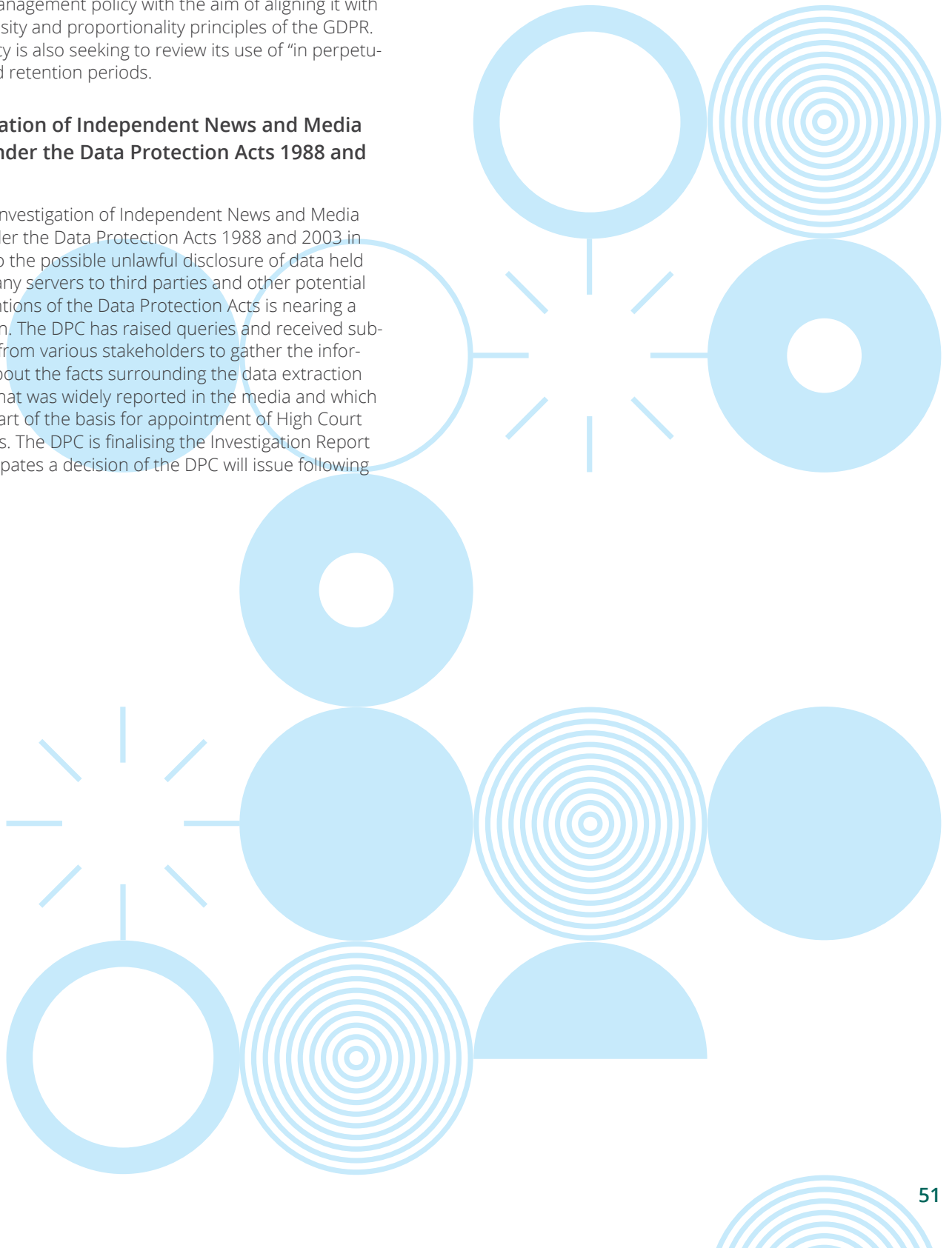
Tusla also confirmed that it expects to revise its current record management policy with the aim of aligning it with the necessity and proportionality principles of the GDPR. The agency is also seeking to review its use of "in perpetuity" record retention periods.

Investigation of Independent News and Media (INM) under the Data Protection Acts 1988 and 2003

The DPC investigation of Independent News and Media (INM) under the Data Protection Acts 1988 and 2003 in relation to the possible unlawful disclosure of data held on company servers to third parties and other potential contraventions of the Data Protection Acts is nearing a conclusion. The DPC has raised queries and received submissions from various stakeholders to gather the information about the facts surrounding the data extraction process that was widely reported in the media and which formed part of the basis for appointment of High Court Inspectors. The DPC is finalising the Investigation Report and anticipates a decision of the DPC will issue following this.

Investigation in relation The Public Services Card under The Data Protection Acts, 1988 and 2003.

A detailed report of the Investigation by the DPC into the processing of personal data by Department of Employment And Social Protection (DEASP) in relation to the Public Services Card can be found in Appendix 3 on page 93.



7

Legal Affairs



Procedural law issues

The work of the DPC's Legal team has always been challenging and diverse but perhaps never so much as during 2019. The progression of the first inquiries, particularly those concerning cross-border processing issues, towards completion has given rise to novel and highly complex issues, including a certain level of procedural challenges being raised by respondent data controllers, as well as individual complainants and (Article 80) representative bodies. These challenges often concern novel points of law, particularly concerning the interaction between the GDPR and the Irish national implementing legislation, the Data Protection Act 2018, which have not previously arisen under Irish law.

During 2019, the DPC has had to consider a multiplicity of legal procedural issues raised by parties to processes conducted by the DPC such as: how best to balance the rights and entitlements of the parties concerned in the context of requests for access to the inquiry file; claims of legal privilege, confidentiality and commercial sensitivity made over material submitted by parties to inquiries; as well as challenges to the fairness of the processes and procedures undertaken by the DPC. In order to determine the various issues arising, the DPC has had to consider how legislative provisions might be interpreted and operated in harmony with European legislation as well as how rights deriving from the European Union's legal framework, such as the right of access to the file and the right to good administration, should operate in the context of an Irish regulatory inquiry. Similarly there

have been many issues arising concerning the potential conflict of other national administrative laws (insofar as they implement and give further effect to the GDPR at national level) with the Data Protection Act 2018. This phenomenon is one which is occurring in the context of the work of supervisory authorities across the EU. Consequently, at EDPB level, supervisory authorities continue to work through how to resolve these procedural issues at a practical level to ensure the highest degree possible of harmonisation of GDPR implementation nationally. The DPC anticipates that 2020 will involve the reconciliation of many such complex legal issues which will flow from the conclusion of its first waves of statutory inquiries (particularly those which must progress to final resolution under the One Stop Shop mechanisms i.e. where the DPC is the Lead Supervisory Authority) and the crystallisation in practical terms of many theoretical legal and procedural issues which have been raised during those first novel inquiries.

Litigation involving the DPC

Between 1 January and 31 December 2019, substantive judgments on data protection issues were delivered in the following proceedings, to which the DPC was a party. It should be noted that these proceedings related to the performance of the DPC's functions under the previous legislative regime of the Data Protection Acts 1988 and 2003.

An appeal to the Circuit Court in the case of *Young's Garage v The Data Protection Commissioner* (judgment of *Nenagh Circuit Court*, delivered 4 February 2019). Note: this judgment was reserved and subsequently delivered orally only and the below is a summary of that oral judgment).

This case concerned an appeal, brought by a car dealership, against a decision of the DPC dated 21 December 2017 in relation to a complaint made by an individual against that dealership. In his complaint, the individual alleged that the dealership provided his personal data to a third party bank for the purpose of enabling the carrying out of a credit check on the individual with that bank. The individual alleged that this credit check, and the processing of his personal data by the dealership for this purpose, took place without his consent.

The DPC commenced an investigation into the complaint, during the course of which the dealership asserted that the individual had consented to the processing of his personal data for the purpose of a credit check. While the dealership asserted that it normally records an individual's consent by way of a "ticked" checkbox on an

application form, the application form relating to the complainant individual did not contain a "ticked" checkbox. In the circumstances, the dealership had no way of proving by way of documentary evidence that the individual had, in fact, consented to the processing of his personal data for the purpose of a credit check. Accordingly, the DPC

found that the dealership breached Section 2A of the Data Protection Acts, 1988 and 2003.

The DPC's decision noted that Section 2A of the Data Protection Acts, 1988 and 2003 requires consent to be "freely given, specific, informed and unambiguous". As the checkbox on the form used to process the individual's personal data had not been "ticked", and there was no further documentary evidence available to support the assertion that the individual consented to the processing, the DPC concluded that the requisite elements of 'consent' were not satisfied in this case and the dealership could not show that it had a lawful basis to support the processing of the individual's personal data. The issue of controllership was also raised by the dealership during the DPC's investigation with the dealership claiming that it was not the controller and instead was a processor for the third party bank to whom the complainant's personal data had been passed. This argument was not accepted by the DPC.

The dealership appealed the decision to the Circuit Court. In the oral judgment delivered by the Circuit Court, the

Court found that the investigation process, as carried by the DPC, had been properly conducted and noted that there were two different accounts of the facts put forward by the dealership and the complainant. The Court found that the DPC's decision was correct based on the evidence before her. On the consent issue, the Court noted that the affidavit sworn on behalf of the dealership in this appeal was silent on the issue of consent and that no evidence had been put forward as to consent having been provided by the complainant to his details being forwarded to the bank. Further, in relation to the question of controllership, the Court found that there was no question but that the dealership was a data controller, and that it was clear that the dealership could not be a processor as it did not act for the bank in question. It was noted that the dealership's solicitor had previously seemed to agree with this position in earlier correspondence; therefore it seemed to follow that the dealership's solicitor accepted that it was not a processor, and it also followed from this that the dealership was a data controller. Therefore the Court did not allow the dealership's appeal.

**An appeal to the Circuit Court in the case of Doolin v The Data Protection Commissioner (judgment of Dublin Circuit Court, delivered 1 May 2019).
Note: the judgment in this appeal was delivered ex tempore only and the below is a summary of that judgment).**

This case concerned an appeal, brought by an individual, against a Decision of the DPC dated 27 July 2018. In the complaint that formed the basis for the Decision, the individual alleged that his employer used CCTV footage of him to sanction him for taking unauthorised breaks at work.

During the course of the investigation, it was established that the employer discovered a threatening message carved into a table in the break room at the place of employment. The employer reported the matter to An Garda Síochána for investigation. An Garda Síochána requested the employer to examine all fob usage records and CCTV footage from a corridor leading to the break room in question. The CCTV footage was used to identify those persons who entered/left the break room. The employer then interviewed the identified members of staff with a view to establishing whether or not the message was on the table during the time they were present in the room (so as to narrow down the time that the incident could have taken place). The employer advised that a number of staff, when interviewed, admitted that they had been taking an unofficial break from their duties. The employer asserted that disciplinary action was taken on the basis of those admissions and that the CCTV footage was not used for the purpose of the disciplinary hearing. The employer reiterated that the only purpose for the use of the CCTV was the investigation into a criminal matter that had been referred to An Garda Síochána.

The individual alleged that the employer breached Section 2 of the Data Protection Acts, 1988 and 2003 ("the Acts") when it used the CCTV footage for disciplinary purposes. The individual relied on the employer's CCTV policy, in this

regard, which stated that the purpose of the CCTV system was to prevent crime and promote staff security and public safety.

In examining the individual's complaint, the DPC considered two issues relating to the processing of his personal data by way of the CCTV system, as follows:

1. Whether the employer had a lawful basis under Section 2A of the Acts for processing the individual's data; and
2. Whether the employer complied with the statutory requirements set out in Section 2(D) of the Acts in relation to the fair processing of the individual's data, with particular reference to the requirement to provide notice of the processing of the individual's personal data.

The DPC firstly noted that it was apparent from the investigation that the employer had a legitimate justification to access and view the CCTV footage in order to make enquiries as to who had carved the offensive and threatening material into the table of the staff break room. It was a serious security issue which potentially gave rise to a threat to staff and it had to be investigated. This included the necessity to view CCTV footage as part of the investigation. Under Section 2A(1)(d) of the Acts, the processing of personal data is permitted if it is necessary for the

purposes of the legitimate interests of the data controller, except where that processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms of the individual.

The DPC had regard to the Opinion of Advocate General Bobek in the Rīgas regional security police case (Case C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme'*) and, in particular, AG Bobek's consideration of the scope and meaning of the term 'legitimate interests'. AG Bobek noted that, when considering whether the 'legitimate interests' ground applies, a three-step test must be followed:

1. There must be the existence of a legitimate interest justifying processing;
2. That interest must prevail over the rights and interests of the individual; and
3. The necessity of processing of the personal data for the realisation of the legitimate interests.

Applying the above to the matters established during the course of the investigation, the DPC was firstly satisfied that the employer demonstrated that it had a legitimate interest in processing the individual's personal data by viewing the CCTV footage in order to identify the staff members who should be interviewed in relation to the security risk presented.

In relation to the second and third limbs of the test, the DPC found that the viewing of the CCTV footage was a crucial investigative step in order to identify the staff members who were present around the time that the incident occurred. The DPC was satisfied that the processing of the individual's personal data in the form of a limited viewing of the relevant CCTV footage, without downloading or further processing of any kind was necessary for this purpose and did not go beyond the stated purpose. The CCTV camera was located outside the staff room and was not monitoring employees in a private area. The DPC therefore concluded that the viewing was proportionate in all of the circumstances and prevailed over the individual's rights and interests in that limited context.

Accordingly, the DPC found that the employer had a lawful basis, under the legitimate interests provision set out in Section 2A(1)(d) of the Acts, for the very limited processing of the individual's personal data which took place in this case.

The DPC further considered whether the requirements of Section 2(1)(c)(ii) of the Acts had been satisfied by the employer. This provision requires that personal data must not be processed for purposes other than the purpose for which it was originally collected. In this case, the DPC was satisfied that the individual's images, as captured on the CCTV system, were processed in connection with the investigation of a security incident when they were

initially viewed by the investigation team for that purpose alone. The information gathered from that viewing may subsequently have been used for another purpose, i.e. disciplinary proceedings, but this, in the view of the DPC, did not constitute a different purpose, because the CCTV images were not further processed for that second purpose. If the images had been further processed for that second purpose, for example by downloading and use in the disciplinary proceedings, it may constitute further processing for a different purpose. This did not occur in this particular case and no further processing of the individual's images occurred for the second purpose. Accordingly, the DPC found that the limited viewing of the individual's images took place exclusively for the security purpose for which the images were originally collected and that no contravention of Section 2(1)(c)(ii) occurred.

Finally, the DPC considered whether the fair processing requirements set out in Section 2D of the Acts were satisfied by the employer in this particular case. The DPC found that it was evident, from the information provided by both the employer and the individual themselves, that the individual was on notice that CCTV footage was in operation in the employer's premises. This was through information provided in the staff handbook which the employer said was issued to every employee during induction. It was also evident through CCTV signage on display at the premises. Accordingly, the DPC was satisfied that the fair processing requirements, as set out in Section 2D, were satisfied by the employer in this particular case.

In his appeal to the Circuit Court, the individual alleged that the DPC had erred in fact or in law in determining that there was no breach of Section 2 of the Acts by his employer in respect of the CCTV footage. To succeed on this claim, and by reference to the test set out in *Orange Limited v The Director of Telecommunications*, the individual had to establish that there had been a serious and significant error or series of such errors. The Court found that the DPC carried out a significant investigation into the individual's complaint and that the individual had been put on full notice of the employer's position and was given every opportunity to make submissions (and did, in fact, make such submissions). The Court also accepted that there had only been one investigation and not two investigations. The investigation undertaken was based on security concerns arising from the graffiti incident in question and the disciplinary action by the employer against the individual was taken for security purposes.

In all of the circumstances, and taking into account all the facts, the Court was satisfied that the individual did not meet the test as would require the DPC's Decision to be overturned. Accordingly, the Court dismissed the individual's appeal. Costs were awarded to the DPC and to the notice party (the employer).

Note: this Circuit Court decision is now under appeal to the High Court.

8

Supervision



Supervision contact with companies, organisations, policy makers and legislators enables the DPC to better understand the ways in which personal data is processed by controllers and processors, and the actions they take to meet their data protection obligations. It helps the DPC in proactively identifying data protection concerns and, in the case of new products or services, ensuring organisations are aware of compliance obligations and potential problems in advance of the commencement of the processing of personal data.

The DPC received 1,420 general consultation queries during 2019. These queries act as a starting point for much of the DPC's supervision of controllers and processors of personal data, and provides an important insight into the types of issues which could benefit from further engagement and guidance. The sectoral breakdown of these queries is as follows:

Sector	Number	%
Health Sector	194	14%
Law Enforcement Sector	35	2%
Private/Financial Sector	629	44%
Public Sector	472	33%
Voluntary/Charity Sector	90	6%
TOTAL	1,420	

Public Sector

A key focus in 2019 was the promotion of 'Guidelines on the processing of personal data by Elected Representatives under Section 40 of the Data Protection Act 2018' published by the DPC at the end of 2018.

Presentations were made to local councillors at the Association of Irish Local Government annual conference, and to members of the Oireachtas and their staff. The guidelines were also presented to the Local Government Data Protection Officers Network, in recognition of the important role that local councillors provide for their constituents in accessing the services of their local authorities.

The DPC engaged with several local authorities in 2019 on the topic of the processing of personal data in the context of waste management enforcement activities. Activity in the local government sector around waste enforcement took two different forms; one was the development of byelaws that sought to allow for increased sharing of personal data in order to more effectively enforce existing waste legislation, and the other was by way of a pilot project which focused on using Eircodes of households in a particular region in order to focus enforcement activities

in that area. The DPC highlighted the importance of proper stakeholder consultation and full consideration of data protection implications by way of data protection impact assessments (DPIAs) as central to success in this area.

The DPC also continued to engage with several key stakeholders of the national smart meter rollout project, including ESBN, the Commission for the Regulation of Utilities (CRU) and the electricity suppliers. As the implementation of this project is being progressed for public policy reasons, the DPC emphasised the need for a clear statutory underpinning for this complex project, in accordance with the Data Protection Act 2018, and will continue to provide guidance on the data protection implications of the project as it develops.

The National Newborn Bloodspot Screening Programme

In 2019, the DPC stepped up regulatory engagement with the Department of Health to bring to a conclusion the matter of the indefinite retention of the historic archive (pre 2012) of national new-born screening test cards. These cards are used in screening newborn babies for a range of health conditions shortly after their birth as part of the National Newborn Bloodspot Screening Programme. The original indefinite retention policy of the programme was found by the DPC in 2010 to be in breach of data protection law. Following this finding, the DPC directed the various stakeholders to find a resolution to the breach, either by way of establishing a lawful basis for the retention of the archive or its destruction. A protracted period of stakeholder consultation and review within the Department of Health was then undertaken, as well as a period of time during which members of the public were afforded the opportunity to extract their cards from the archive. The DPC has been informed that a Ministerial order for the destruction of the archive has now been signed and we understand the destruction process will be completed in the first quarter of 2020. It should be noted that, following revision of its data retention policy in 2012, the National Newborn Bloodspot Screening Programme as it currently operates does not present any data protection concerns.

Prior Consultation

Under the GDPR and the Data Protection Act 2018, there is a mandatory obligation to consult with the DPC on legislative proposals involving the processing of personal data. In this area we encourage early engagement so that we have a clear understanding of the legislation and what it is trying to achieve at the earliest opportunity. This also allows us to encourage government departments to adhere to the principle of 'data protection by design', and to carry out effective Data Protection Impact Assessments.

In 2019 the DPC was consulted by a range of government departments and other stakeholders on legislative matters including, but not limited to, the following:

Sample of Legislative Consultations:

- Adoption (Information and Tracing) Bill 2016
- Proposals on The Future Funding of Public Service Broadcasting
- Proposals to extend the circumstances in which recording devices, including Body worn cameras, can be used by An Garda Síochána
- Report on the Collection of Tuam Survivors' DNA Publication
- Affordable Childcare Scheme — prescribing persons who may process personal data
- CervicalCheck Tribunal Bill 2019
- Amendments to the Electoral Act 1992 to allow for the establishment of the Citizens Assembly 2019 and the Dublin Citizens Assembly
- The Civil Registration Bill 2019
- Defence Forces (Evidence) Bill 2019
- Disabled Drivers and Disabled Passengers Fuel Grant
- Registrar of Beneficial Ownership of Companies and Industrial and Provident Societies
- Proposal for the Establishment of a Statutory Electoral Commission
- Draft General Scheme of the Sea-Fisheries (Amendment) Bill 2019
- Amendment to the Gaming & Lotteries Act 1956
- Gender Pay Gap Information Bill 2019
- European Union (Hague Maintenance Convention) Regulations 2019
- Housing (Regulation of Approved Housing Bodies) Bill 2019
- Investment Limited Partnerships (Amendment) Bill 2019
- S.I. to establish A Beneficial Ownership Register for ICAVs (Irish Collective Asset-Management Vehicles) and Credit Unions
- S.I. to create a beneficial ownership register for the beneficial owners of Trusts
- Regulations to add the Registrar of Beneficial Ownership of Companies and Industrial and Provident Societies as a specified body to Schedule 5 of the Social Welfare Consolidation Act 2005

- Judicial Council Act 2019
- Microchipping of Dogs Regulations 2019
- Monuments and Archaeological Heritage Bill 2019
- Parental Leave (Amendment) Bill 2017
- Residential Tenancies Amendment Bill 2018
- Data Protection Act 2018 (Section 60(6)) (Health Professionals' Regulators) Regulations 2018
- Amendments to the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018
- Social Welfare Spring Bill 2019
- Transposition of EU Shareholders Rights Directive (providing for the identification of shareholders and remuneration of directors) as amendments to the Companies Act
- Waste Presentation Byelaws

Sample of Non-legislative Observations:

- Public Consultation on the Potential Introduction of Open or Semi-Open Adoption in Ireland
- National Action Plan of Business and Human Rights
- Draft National Risk Assessment 2019 — Overview of Strategic Risks Report
- Revenue Statement of Strategy
- Public Consultation on National Cyber Security Strategy
- EU Commission Survey on Internet Connected radio equipment and wearable radio equipment
- National Artificial Intelligence Strategy
- Public Consultation and launch of updated Central Bank of Ireland guidance, on policies and procedures for entities, in complying with Anti Money Laundering laws
- Proposal for a Fraud Sharing Database in the Banking sector
- Proposal for an Insurance Fraud Database
- Proposal by Dept of Transport Tourism & Sport, to set up a 'Motor Third Party Liability Database', to record the insurance status of registered vehicles

Law Enforcement

Over 2019 the DPC was involved in extensive consultations with An Garda Síochána in respect of its programme to modernise core technology platforms. This included reviewing data protection impact assessments for its Electronic Content Management (ECM) platform and

Investigative Management system (IMS). The DPC also engaged with An Garda Síochána on its data protection impact assessment in respect of the Schengen Information System second generation project (SIS II).

Private and Financial Sector

Supervision of private sector entities and organisations connected with the financial, banking and insurance sectors continued in 2019 providing direction and guidance to data controllers on a broad range of complex data protection issues. The organisations with whom the DPC engaged during 2019 included:

- Ulster Bank
- Bank of Ireland
- Permanent TSB
- Western Union
- Prudential Assurance
- Aer Lingus
- SIPTU
- Irish Rail
- Lidl
- Banking Payments Federation Ireland
- Accountancy Ireland
- Irish Farmers Association
- Money Advice and Budgeting Service (MABS)
- IBEC (Telecommunication and Internet Federation)
- Insurance Ireland
- National Recruitment Federation
- The Irish Association of Pension Funds
- Irish Petrol Retailers Association
- Department of Finance
- Revenue Commissioners
- Central Bank of Ireland
- An Garda Síochána

Whilst it can be seen since the introduction of the GDPR in May 2018 there is greater awareness amongst private sector organisations of data protection obligations and so contributing to the reduction in queries received some of the core recurring concerns for companies throughout 2019, amongst others, included:

- Personal data transfers following a No-Deal Brexit
- Direct Marketing rules under the ePrivacy Directive
- Effectively dealing with Subject Access Requests
- Use of technologies in the workplace such as biometric clocking/GPS vehicle tracking and CCTV in the workplace
- Transferring of employee data in mergers and takeovers
- New technologies and their impact on controller's data protection obligations.

2019 saw continued emergence of new technologies most notably in the Fintech and payments industry with the advent of Open Banking and the European Payment Services Directive 2 (PSD2) with new Fintech start-ups or trusted third-parties (TPPs) setting up operations in Ireland. This is expected to gather momentum in 2020 and as the sharing of account information and personal data is the cornerstone of the Directive this will be a core priority for the coming year for the DPC's consultation engagement with the private and financial sector.

CASE STUDY 13 Proposals for Fraud Sharing Databases

During 2019 the DPC was consulted on proposals for the creation of two separate fraud information-sharing databases.

The first proposal from Insurance Ireland is to expand an existing database, called InsuranceLink, to include additional data fields. InsuranceLink contains details of insurance claims made by individuals to facilitate the exchange of information between insurance companies when a claim for compensation has been made by a customer for the purpose of identifying fraud where

false claims are being potentially processed. One of the proposed additional data sets is third party personal data such as witnesses to accidents.

The second proposal was from Banking and Payments Federation Ireland (BPFI) on behalf of the main retail banks, who wish to create a fraud information-sharing da-

tabase that would be operated by an independent trusted third party. Each bank that establishes fraudulent activity would, according to predefined rules, transmit that information to the database and all participant banks would be permitted to check client details against the database for the purposes of identifying and preventing fraud.

The DPC has emphasised to both Insurance Ireland and BPI that industry fraud databases, involving the processing of significant volumes of sensitive data, must meet necessity and proportionality requirements under EU law and jurisprudence. We have also emphasised that the operation of each database must, as necessary, have a statutory underpinning to ensure compliance with data protection obligations under the GDPR and the Data Protection Act 2018, such as, for example, where the

processing is in the public interest and/or involves data relating to offences or alleged offences.

It is the DPC's view that both proposals raise significant risks for individuals, in particular to persons who may be wrongly identified as participating in fraudulent activity, or, in the case of insurance claims, to persons who are not directly linked to a claim such as a witness. We have advised the parties that these risks must be fully assessed and mitigated, including by building in very robust safeguards, rules and procedures and ensuring that the principles of data protection such as data minimisation are complied with. Furthermore, we have highlighted the importance of public consultation and awareness on the scope and purpose of these proposals.

Multinational Supervision

In 2019, the DPC attended over 100 meetings with various multinational companies in its supervisory capacity. In addition, the DPC issued formal requests seeking detailed information on compliance with the GDPR on a broad range of matters such as:

- discrepancies in privacy policies;
- media reports outlining security issues, e.g. human review of voice recordings;

- seeking improvements to processing activities such as location tracking;
- reviewing potential new features and products, e.g. a suicide & self-harm prevention feature; and
- assisting our European counterparts in relation to concerns raised by them, e.g. the use of diagnostic data.

Certification and Codes of Conduct

Certification

During 2019, the DPC continued with its preparation for the implementation of the GDPR's certification approval mechanisms. GDPR certification is intended as an accountability mechanism for organisations' specific processing operations, to demonstrate compliance efforts to individuals and ultimately to support individuals' trust in personal data processing.

The GDPR allows for the Supervisory Authority or the member state's National Accreditation Board (NAB) to accredit certification bodies to "data protection certification mechanisms" in accordance with ISO 17065/2012 and with additional requirements established by DPC. Section 35 of the Irish Data Protection Act, 2018, sets out that the Irish National Accreditation Board (INAB) will be the sole accrediting body for Ireland. As a result, the DPC will not be undertaking the role of an accreditation body in Ireland.

As part of implementing Article 43 of the GDPR, the DPC must set out "additional requirements" to that of ISO 17065/2012 that INAB will apply during accreditation of certification bodies to certification mechanisms that have DPC approved data protection criteria. The DPC have just finalised these additional requirements which are now to be submitted to the EDPB in the early part of 2020. These will be subject to an EDPB consistency opinion. Once this opinion is adopted by the EDPB and any adjustments accounted for by the DPC they will be made publically available.

The DPC is also currently in the process of finalising a co-operation agreement with INAB, regarding accreditation operations. Work has also commenced on the operational aspects of assessing schemes' data protection criteria that stakeholders may submit to DPC and on the detailed communication, cooperation and interaction the DPC will have with INAB, scheme 'owners', and the EDPB during the approval process.

Finally, in late 2019, the DPC co-hosted with INAB an initial information session with a group of certification bodies and other stakeholders to raise awareness of the parameters of GDPR certification mechanisms and to encourage development of such mechanisms among certification bodies. This was the first in a series of information sessions with further expected to take place in 2020.

Codes of Conduct

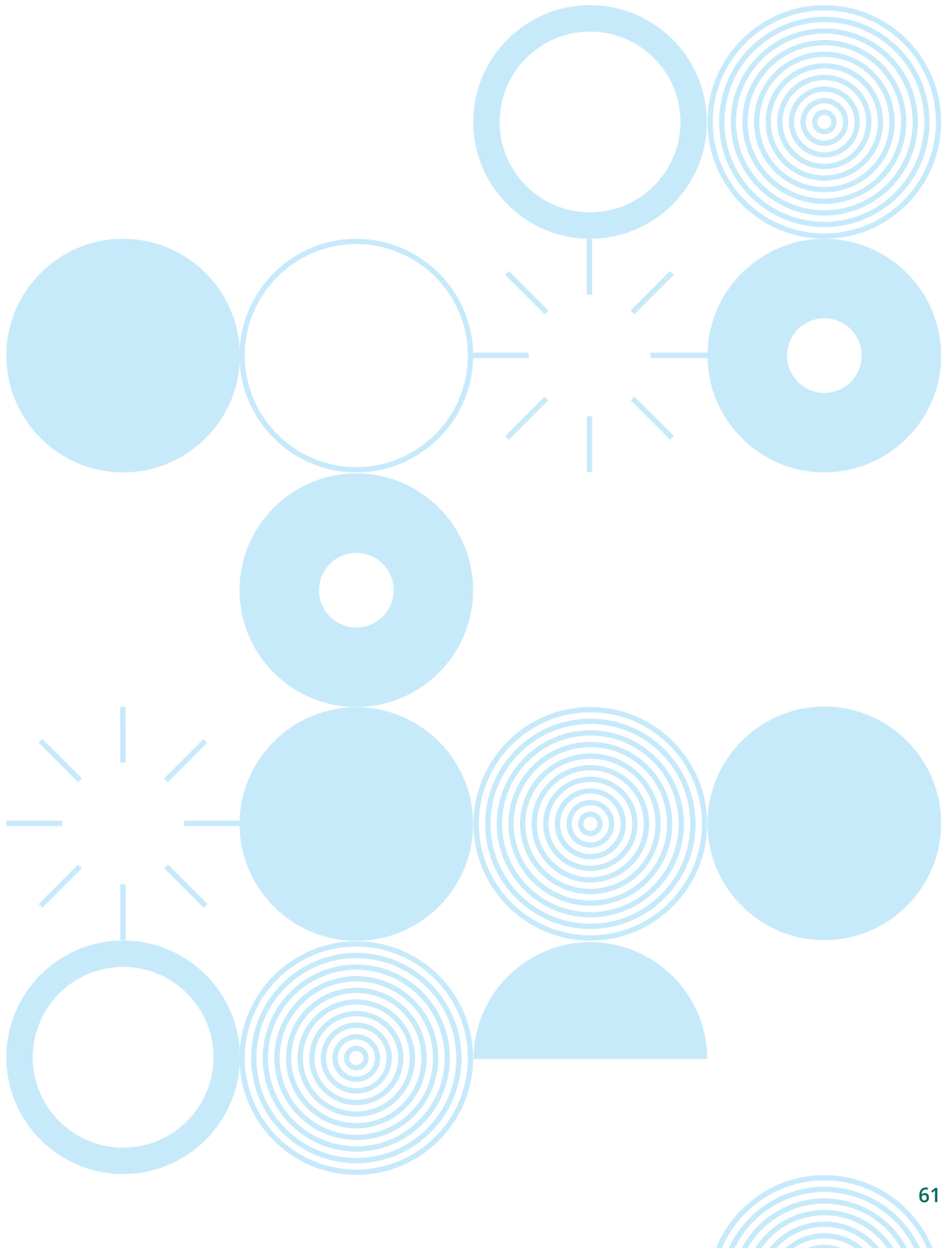
Rules around the drafting and monitoring of 'Codes of Conduct' are set out in Articles 40 and 41 of the GDPR, representing a practical and meaningful method of achieving greater levels of compliance with the principles of data protection and of protection for data protection rights. Codes of Conduct can, in particular, provide an opportunity for specific sectors to reflect upon common data processing activities and to agree to context-specific and practical rules and procedures, which will meet the needs of the sector as well as the requirements of the GDPR.

The DPC led on the development of EDPB guidelines on the drafting of Codes of Conduct and appointing Monitoring Bodies for those Codes, as set out by the GDPR, which

were approved and published by the EDPB in June 2019, following public consultation. The DPC has compiled draft accreditation criteria for the accreditation of Monitoring Bodies which will be tasked with monitoring compliance with any proposed Codes of Conduct. The review of these criteria by the EDPB and their approval and publication in 2020 will be an important step towards supporting organisations in drawing up Codes of Conduct, alongside the previously published EDPB guidelines.

The DPC looks forward to the development of Codes of Conduct as a way to improve standards of data protection and transparency for particular sectors or processing

operations. Codes of Conduct, properly monitored by suitable Monitoring Bodies, will bring more comprehensive, context-specific clarity to the data protection obligations of certain sectors and certain controllers. Following the extensive consultation work undertaken by the DPC in the area of children's data protection rights, the DPC will encourage the drawing up of Codes of Conduct intended to contribute to the proper application of data protection to the processing of children's personal data (more information on the Children's' Consultation can be found on page 66).



9

Data Protection Officers



DPC's DPO

The Data Protection Officer (DPO) of an organisation is a person with expert knowledge of data protection law and practices. Their role is to help the organisation monitor compliance with the GDPR. It is essential that the DPC, as the Irish regulator for data protection, meets the highest standard of data protection compliance in respect of the personal data it processes.

The GDPR requires the appointment of a DPO with the necessary professional qualities and, in particular, refers to expert knowledge of data protection law and practice. As a qualified solicitor with experience in ensuring practical compliance with data protection obligations from an organisational perspective, the DPC's DPO has the required expert knowledge of data protection law. In addition, as a senior member of staff of the DPC (Assistant Commissioner), the DPC's DPO reports directly to the highest level of management of the DPC (its SMC), as required by the GDPR.

The role of the DPO in a data protection supervisory authority such as the DPC is broadly similar to the role of the DPO in any other data controller. It can involve responding to subject access requests and other queries from members of the public. The DPO also responds to queries from DPC staff members and ensures security measures and data protection policies are relevant and up-to-date. The DPO ensures that the Record of Processing Activities is accurate and provides assistance to the DPC with Data Protection Impact Assessments. The DPO also advises on some of the DPC's wider strategic projects, such as the DPC's Accounting Officer Project.

In November 2019, the European Data Protection Board set up its own DPO Network to bring together the DPOs of all EU data supervisory authorities, to discuss the specific and unique aspects of the DPO role in these organisations. As a member of this network, the DPC's DPO has an opportunity to share knowledge and develop best practices with the DPOs of other data supervisory authorities with the objective of implementing a coordinated and consistent approach to compliance with the GDPR.

The DPC's DPO acts as a 'critical friend' to the DPC. By identifying key data protection issues, understanding the legal matrix, the operational context, measuring risk and proactively taking proportionate action when required, the DPC's DPO not only serves the cause of data protection, but also addresses organisational-risk exposure from multiple perspectives.

The DPC's DPO can be reached via dpo@dataprotection.ie.

DPO Notifications to the DPC

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 2019, the DPC received 712 DPO notifications through the online webform on the DPC website. The table below shows the industry sectors from which notifications were made.

DPO notifications for 2019

Private	577
Public	49
Not-for-Profit	86
Total in 2019	712

Engagement with DPOs

The DPC is committed to engaging fully with DPOs and their teams, in recognition of their key role in ensuring that the progress made to date in implementing GDPR programmes translates into lasting organisational culture and practice. DPC staff spoke at many events for DPOs during the year and a DPC-facilitated DPO Network was developed in late 2019. Mobilising this Network is a priority for the DPC for 2020. The purpose of the Network is to foster peer-to-peer engagement and knowledge-sharing between DPOs. The first initiative being rolled-out by the DPC for this Network is a DPO conference on 31 March 2020, with further initiatives such as webinars, regional events and the publication of further guidance planned.

10

International Activities



International Transfers

A key focus in the area of international transfers for the Data Protection Commission is the assessment and approval of Binding Corporate Rules applications from multi-national companies. It also has an advisory role on general transfers matters; attending events and speaking engagements and meetings of the International Transfers expert subgroup of the European Data Protection Board (EDPB).

Binding Corporate Rules

Binding Corporate Rules (BCR) were introduced in response to the need 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. The inclusion of BCR in the GDPR further solidifies their use as an appropriate safeguard to legitimise transfers to Third Countries.

During 2019, the DPC continued to act or commenced acting as lead reviewer in relation to 19 BCR applications from 12 different companies.

The DPC also assisted other European Data Protection Agencies (DPA's) by acting as co-reviewer on 5 BCRs in this period.

The procedure for approval of BCRs has changed from a system of mutual recognition under the Directive to the current system, where all BCRs must be submitted to the EDPB for an Article 64 opinion. This process means all DPAs get an opportunity to comment on all BCR applications, which results in a slightly longer co-operation procedure. This procedure will assist the EDPB in drafting its opinion if all issues are dealt with in advance of the Article 64 procedure.

The EDPB issued Article 64 opinions on 2 BCR applications submitted through the UK and Belgian DPAs in 2019. We expect to seek similar opinions on a number of DPC-led BCRs in the first quarter of 2020.

Due to the upcoming departure of the UK from the European Union, we have had contact from a number of companies enquiring about moving their lead authority for BCR purposes to the DPC. It is expected that the numbers of BCRs that the DPC will handle will increase in 2020, once the UK has left the EU and those companies with an ICO-approved BCR need a new BCR lead authority.

Brexit

In 2019, the DPC spent a lot of time engaging with stakeholders and providing information on Brexit, particularly the impact on Irish companies transferring personal data to the UK in the event of a no-deal Brexit. The DPC participated in joint events with IBEC, Enterprise Ireland and

Local Enterprise Boards to ensure that information was delivered to as many companies as possible. The main concern was that smaller companies who did not routinely transfer data to third countries could be in contravention of the GDPR if they continued to do so post-Brexit without applying the relevant safeguards to the transfer.

The DPC also directly advised and participated in events within the public sector to give advice which could be used in the event of the UK becoming a third country from the point of view of data transfers.

Other International Transfer Issues

Staff from the DPC attended 7 meetings of the EDPB International Transfers expert sub-group (ITES) in 2019. This sub-group of the EDPB meets to consider, advise and prepare documentation on matters concerning International Transfers.

DPC's EU Role

During 2019, the DPC continued to play a central role in safeguarding the data protection rights of millions of people across the European Economic Area (EEA).⁶ The DPC holds these increased responsibilities arising from the cooperation and consistency mechanisms under the GDPR.

Consistency Mechanism and EDPB Tasks

Like all other EEA data protection supervisory authorities, the DPC must ensure that we interpret, supervise and enforce the GDPR in a way that achieves consistency. The GDPR's consistency mechanism introduced several additional tasks for the EDPB and all of its members, including the DPC, to ensure that the goal of harmonisation is reached.

These tasks are mainly delivered through the work of the EDPB's expert subgroups and plenary meetings, in which the DPC participates fully, given the importance of these tasks. During 2019, DPC staff members attended over 80 in-person meetings in Brussels related to EDPB activities, including those of the twelve EDPB expert subgroups:

- Borders, Travel and Law Enforcement;
- Cooperation;
- Compliance, eGovernment and Health;
- Enforcement;
- Financial Matters;

⁶ The European Economic Area includes all European Union (EU) member states and Iceland, Liechtenstein, and Norway.

- Fining Taskforce;
 - International Transfers;
 - IT Users;
 - Key Provisions;
 - Social Media;
 - Strategic Advisory; and
 - Technology.

DPC staff members have contributed extensively to the development of guidelines and opinions across all of the EDPB expert subgroups during 2019. The DPC is the co-ordinator of the Social Media expert subgroup and was co-rapporteur of that subgroup's work on regulatory priorities relating to the processing of personal data by social media companies, in the past year.

During 2019, the DPC hosted counterparts from the UK, Iceland, the Netherlands, Luxembourg and Sweden, and visited colleagues in the UK, Germany and Belgium. These bilateral discussions and exchange of experiences have been very valuable towards ensuring consistency. These meetings will continue in 2020.

European Data Protection Supervisory Bodies

During 2019, the DPC continued to actively 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. In addition, we continued to participate as observers to the coordinated supervision of the Schengen and Visa Information Systems (SIS II and VIS).

With regard to SIS II, during the course of 2019, the DPC continued to work alongside An Garda Síochána and the Department of Justice & Equality in relation to Ireland's imminent participation in certain non-border aspects of the Schengen acquis and connection to SIS II. The work programme to progress Ireland's participation will continue in 2020.

Other European Engagement

Representatives of the DPC spoke at conferences and events in many EEA Member States during 2019, including Belgium, Germany, France, the UK and Slovenia. Several DPC members of staff participated in the annual case-handling workshop for European data protection supervisory authorities, from both EEA and non-EEA countries, which was hosted by the European Data Protection Supervisor (EDPS) in Brussels in November. We were also very pleased to host a colleague from the Rhineland-Palatinate supervisory authority, who spent a week at the DPC in October.

In December 2019, the DPC signed up to a two-year programme in collaboration with our Croatian counterparts and Vrije University Belgium, mainly funded by the EU Commission. The aim of the programme is to increase the awareness, knowledge and understanding of Small-Me-

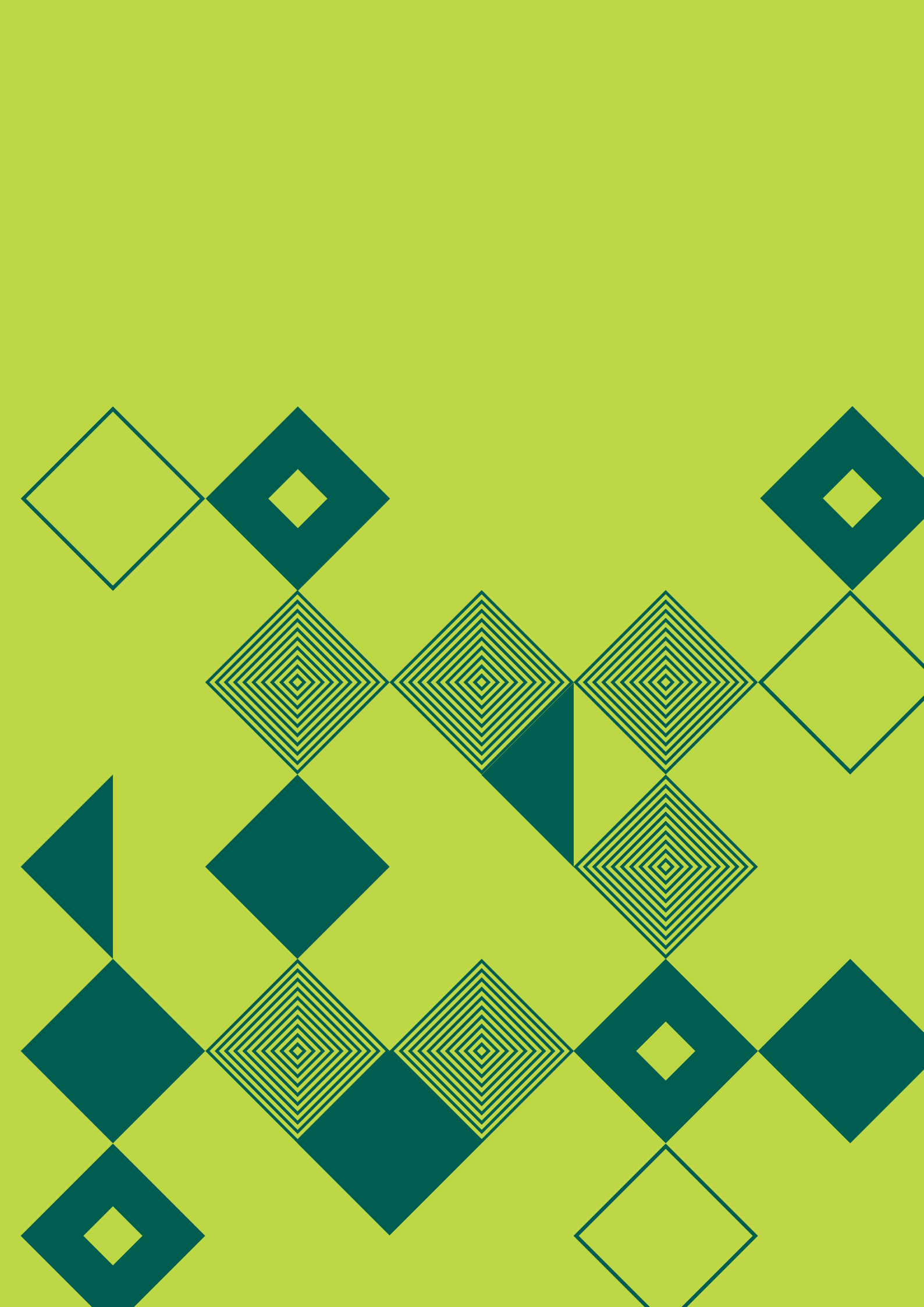
dium Enterprises (SMEs) in Europe, on the principles of data protection, so that their future compliance levels are strengthened. The programme will start in early 2020.

International Engagement

The DPC engages with supervisory authorities, international organisations and legislators from outside of the EU, to share information on the DPC's practices and experiences. This engagement helps to ensure that our own regulatory approach is understood, and it also helps us to understand the differences in regulatory approach in other countries, including in how this affects people and organisations.

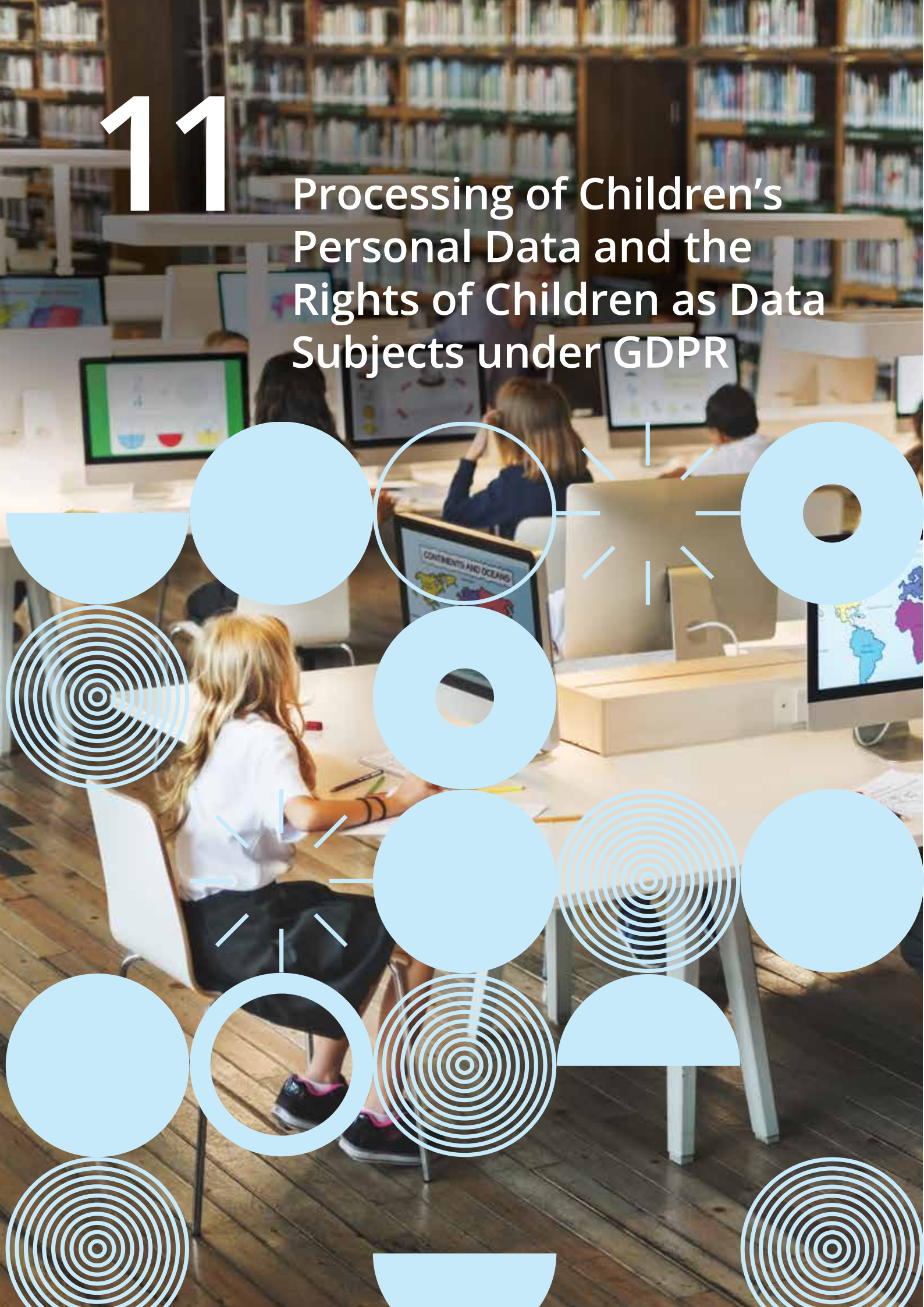
The Commissioner appeared before the US Senate Committee on Commerce, Science and Transportation in May, as part of the Committee's examination of consumer expectations on data privacy. She also appeared before the International Grand Committee on Disinformation and 'Fake News' at its hearing held in Dublin in November, attended by parliamentarians from ten countries. The DPC hosted delegations throughout the year from countries including Australia, New Zealand and the United States, amongst others.

Also as part of this activity, senior DPC staff attended the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Tirana, Albania, which took place in October. The ICDPPC is a global forum for data protection authorities to share knowledge and insights. Following the conference, the name of the ICDPPC forum was changed to the Global Privacy Assembly (GPA). The DPC also attended the meeting of the British Isles and Islands Data Protection Authorities (BIIDPA) in Jersey June 2019. The DPC will host the next BIIDPA annual conference in Dublin in June 2020.



11

Processing of Children's Personal Data and the Rights of Children as Data Subjects under GDPR



Processing of Children’s Personal Data and the Rights of Children as Data Subjects under the GDPR

Background

In 2018, the DPC launched an initiative as part of the DPC’s obligation under the GDPR to promote awareness and understanding of issues concerning the processing of children’s personal data, the specific standards required for the protection of children’s personal data, and the rights of children as data subjects. Following exploratory work in early 2018, it became clear that the significance attributed to children under the GDPR meant that a special consultation to gather the views of all relevant stakeholders, most importantly children themselves, was required.

Launch of the consultation

The DPC’s public consultation on the processing of children’s personal data and the rights of children as data subjects under the GDPR ran from December 2018 to April 2019. It focussed on several questions that the DPC wished to put to the public on the interpretation of key provisions in the GDPR in relation to children.

The consultation was divided into two streams:

- Stream 1, launched in December 2018, targeted adult stakeholders and invited all interested parties — including, parents, educators, children’s rights organisations, and others — to submit their responses to any or all of the 16 questions set out in the consultation document that was published on the DPC’s website.
- Stream 2 was launched on International Data Protection Day (28 January 2019) and sought to involve children and young people directly in the classroom through an innovative and specially designed lesson plan and consultation process.

The DPC reached out to every primary and post-primary school in Ireland — as well as all Youthreach centres — informing them of the consultation and inviting them to take part. The DPC distributed a pack of lesson plan materials that had previously been tested, with the support of the Ombudsman for Children’s Office (OCO), in a series of pilot workshops in October 2018. The lesson plan was designed to help teachers discuss data protection issues with their students and had a particular focus on data protection in the context of social media. It introduced students to “SquadShare”, a fictitious app created by the DPC for educational purposes, and encouraged them to explore their data protection rights while learning about the terms and conditions of this fictitious app. Students were then invited to give their answers to a series of six questions on feedback posters and return them to the DPC via email and post.

Feedback and preliminary reports

In total, the DPC received 30 submissions from adult stakeholders including technology and social media companies, children’s rights charities, public sector bodies, academia and trade associations. Stream 2 of the consul-

tation gathered the views of approximately 1,200 children and young people across Ireland. It was very encouraging to see both streams of the consultation generate such a high level of interest. Adult stakeholders were well represented across all sectors and children were well represented across all age groups, which were also very positive developments.

The DPC spent several months following the close of the consultation analysing the submissions of all respondents. Two preliminary reports, each focusing on a separate stream of the consultation, were published in July and September 2019 (called “Some Stuff You Just Want to Keep Private!” and “Whose Rights Are They Anyway?”). Each report presented qualitative and quantitative trends observed across all responses to the consultation and the DPC’s interpretation of these results. The consultation has to date received considerable praise and recognition. It was cited by the ICDPPC Digital Education Working Group (DEWG) as a core international initiative under the DEWG’s Action Plan for “*Awareness-raising on the exercise of digital rights by the children themselves*”. It was also short-listed as one of two finalists in the Education and Public Awareness category of the 2019 ICDPPC Awards for its child-focused consultation initiative.

Next steps

The DPC is now finalising its guidance document on children’s data protection rights and the processing of children’s data. This is intended to be a guide for data controllers and interested parties on how to address the issues highlighted in the DPC’s consultation, taking into account the feedback from participants. Specifically, this guidance will shed light on the following questions:

- How and when should children be able to exercise their data protection rights for themselves and the role of parents or guardians in this regard?
- What information should be given to children about the use of their personal data?
- How the age of digital consent should be implemented for processing based on consent?
- Under what circumstances is the profiling of children for advertising or marketing purposes permissible?

The DPC plans to publish this guidance in early 2020 and will run a further public consultation on this document to take account of the views of stakeholders before finalising it.

In tandem with the guidance, the DPC will be publishing a separate child-friendly guide which will explain to children their rights under data protection law and the risks that may arise when they disclose their personal data online. Finally, the DPC will also work with industry, government and voluntary sector stakeholders and their representative bodies on foot of the consultation to encourage the drawing up of codes of conduct in relation to the processing of children’s personal data, as per Section 32 of the Data Protection Act 2018. Working towards the development of codes of conduct in this area is a priority for the DPC in 2020.

12

Communications



Direct Engagement

The DPC continued an active outreach schedule during 2019 engaging with a broad base of Irish and international stakeholders. The Commissioner and her staff spoke, presented or otherwise contributed at events on over 180 occasions during the year. For example:

National:

- Research report launch of 'Falling Through the Cracks';
- PDP 2019 Annual Data Protection Conference;
- Taking Care of Business 2019;
- National Association of Principals and Deputy Principals Data Protection Seminar;
- Digital Summit 2019;
- IIEA Young Professionals' Network;
- Early Childhood Ireland Annual Conference;
- NSSO Annual Conference; and
- UCD Student Legal Convention 2019.

Parliamentary Committees (Oireachtas):

- Joint Committee on Justice and Equality;
- Committee of Public Accounts;
- Joint Committee on Communications, Climate Action and Environment; and
- International Grand Committee on Disinformation and Fake News.⁷

International:

- AmCham 7th Annual Transatlantic Digital Economy Conference;
- Technology Law Committee of the International Bar Association — 6th Biennial Technology Law Conference;
- The Eurofi Financial Forum 2019;
- Sooner than you think — A Bloomberg technology series;
- International Association of Privacy Professionals Summit Washington DC; and
- IAPP Congress Brussels.
- United States Senate Committee on Commerce, Science and Transportation.

Media engagement

The profile of, and the media interest in, the DPC continued to grow at both national and international level during 2019. Domestically, the Commissioner and other senior staff appeared on national television, national and regional radio and contributed to print and digital media throughout the year. Much of the media engagement emanated from investigations, e.g. the publishing of the DPC's report into the Public Services Card investigation in August. On other occasions, the DPC engaged in interviews to talk through practical issues that were of public concern/interest such as taking photographs at school events and there was also significant media attention around the DPC's appearances at various Oireachtas Committee hearings throughout the year.

On the international front, the Commissioner and DPC staff engaged regularly with a wide range of media outlets, including Bloomberg, BBC, CNN, Politico, the Wall Street Journal, the New York Times and the Financial Times, to name a few. A large amount of this engagement focussed on the operation of the One Stop Shop and on the statutory inquiries that the DPC has open into multinational technology companies, as well as dealing with breaches and issues that arose in the tech sector during the year. There was also significant international media attention surrounding the DPC's attendance at a US Senate Committee hearing in May 2019.

Guidance, blogs and podcasts

The DPC continued to update, produce and disseminate comprehensive guidance on a wide variety of topics in the form of podcasts, blogs, and formal guidance, for both the public and organisations, to raise awareness of data protection law and its various rights and obligations. In total the DPC published 33 guidance documents, 18 blogs and released 8 podcasts in 2019. This guidance covered general topics, as well as providing more detailed guidance on certain topical or complex issues.

Some of the topics on which the DPC produced guidance during 2019 included:

- the basics of data protection;
- guidance for both organisations and individuals on the use of CCTV;
- guidance regarding requesting personal data from prospective tenants;
- FAQ for individuals on access requests; and
- guidance on the principles of data protection.

Under the GDPR mandatory breach notification regime, receiving, analysing, and acting on breach notifications has been a significant area of growth for the DPC. In light of that, the DPC produced both a 'quick guide' to breach

⁷ *Not an Oireachtas committee, an interparliamentary committee to which the Oireachtas sends delegates. Hosted by the Oireachtas on 7 November.

notification obligations and a more detailed 'practical guide' which provided further practical guidance based on the experiences of the DPC and controllers following the first year of the GDPR.

The DPC also continued to both produce and update technical guidance, focusing mainly on online and digital security, as well as the data protection implications on new and emerging technologies. The DPC published security-focused guidance on phishing and social engineering attacks, portable storage devices, and cloud service providers, as well as a guide to common online risks which individuals may encounter.

In light of developments regarding the UK's planned withdrawal from the EU, the DPC published guidance on international transfers of personal data in the case of a 'No Deal' Brexit scenario and a Brexit FAQ, as well as updating our general guidance on transfers of personal data to third countries or international organisations.

The production and dissemination of podcasts and blogs were a key element of the DPC's external communications strategy for 2019, with a regular podcast 'Know Your Data', as well as a series of myth-busting and topical blogs, shedding light on areas of interest to the general public, as well as highlighting relevant guidance published by the DPC. Topics covered included:

- Does the GDPR Really Say That?;
- Taking photos at school events;
- Video surveillance in the home;
- What to do if you find personal data in a public place?;
- Representing account-holders; and
- Christmas myth-busting blog.

EDPB Guidance

The DPC also worked closely with our fellow data protection authorities through the EDPB to produce guidance documents on EU data protection law. During 2019, the EDPB published guidelines and draft guidelines on topics including:

- Codes of Conduct and monitoring bodies;
- Video devices;
- Data protection by design and by default; and
- The right to be forgotten and search engines.

Links to EDPB guidelines and publications are also available on the DPC website.

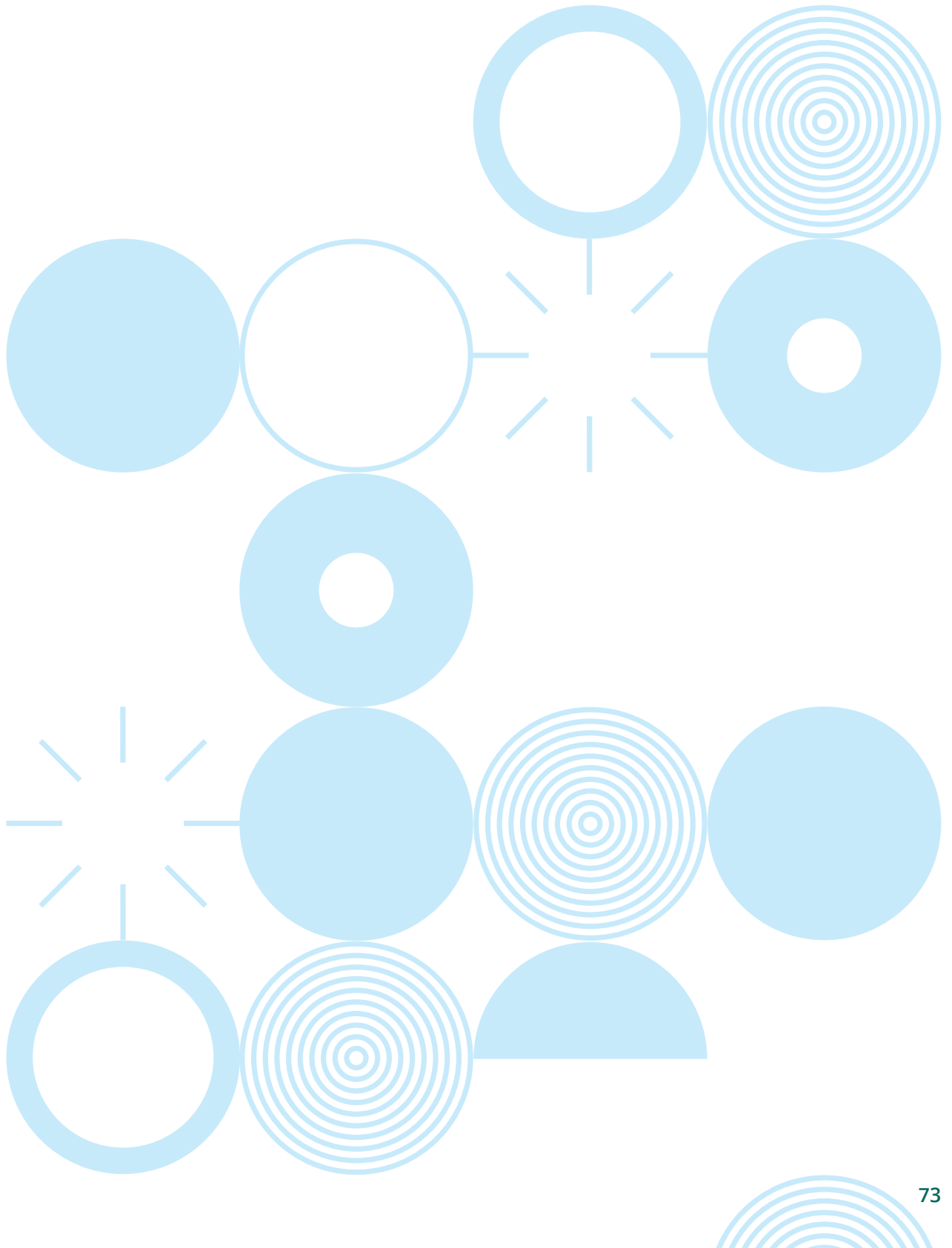
Social media

The DPC has continued to utilise social media in support of its awareness-raising and communications activities. In 2019, the DPC continued to grow its social media activities across Twitter, Instagram and LinkedIn. Our combined followers across the three platforms has more than doubled, exceeding 20,000 by the end of 2019. There was an organic reach of almost 3.3 million, reaching hundreds of thousands of accounts each month.

The DPC has continued to enhance its engagement on social media through producing visually impactful infographics, videos and gifs, which have been effective tools in disseminating guidance and supporting the DPC's awareness-raising activities.

DPC Website

The DPC website, www.dataprotection.ie, is an important resource for individuals and organisations. The DPC's webforms provide website users with a convenient means of submitting complaints, breach notifications, and general queries directly to the DPC. In addition to press releases and statements, guidance, blogs and podcasts on topical issues of relevance to our stakeholders were published frequently throughout 2019.



13

Key DPC Projects



Regulatory Strategy 2020–2025

Work on the DPC's new Regulatory Strategy, for the period from 2020 to 2025, continued during 2019. This project is an opportunity to re-examine how our work could have the biggest impact possible within the resources we have available to us, taking account of the greatest risks to people's rights. It also ensures we consider how we can best set ourselves up to deliver that impact over the next five years even while our regulatory environment continues to change, from the point of view of changes in society, technology, law and the EU.

As part of our analysis of the context in which we regulate, we commenced two main consultation initiatives during 2019. The first consultation exercise was run in July 2019 and involved a series of focus groups with members of the public. The purpose of these focus groups was to:

- understand people's views on data protection rights;
- the role of the DPC;
- how compliance with data protection law should be encouraged, facilitated and maximised; and
- how non-compliance should be regulated.

The key output from this first consultation was a document on the DPC's Target Outcomes. This document focuses on the target outcomes to which we aspire and on how the DPC's activities help to achieve those outcomes.

The second key consultation exercise during 2019 was the open public consultation on the DPC's Target Outcomes, which commenced in December and ran until the end of January 2020. The submissions received are now being analysed as part of the development of the draft Regulatory Strategy itself. The draft Regulatory Strategy will then be subject to a further open public consultation during 2020. We may also consult directly with representative bodies, advocacy groups and other organisations.

A Strategy Implementation and Measurement Plan will also be published, later in 2020, which will set out how the strategic priorities will be implemented through key projects and initiatives. This Plan will also set out how the impact to our target outcomes will be measured.

In line with our Public Sector Equality and Human Rights Duty, our Regulatory Strategy will set out, in a manner accessible to the public, the human rights and equality issues which are relevant to the work of the DPC and our proposed plans to address these issues.

DPC Accounting Officer

Up to and including 2019, the DPC's funding has been included within the budget of the Department of Justice and Equality (DJE), with that budget being voted on each year by the Dáil; that is, the DPC has been included in the DJE's Vote until now. The Accounting Officer remit of the Secretary General of the DJE has therefore included the DPC's expenditure to date, in terms of holding accountability for the regularity and propriety of expenditure in the DJE's Vote, for economy and efficiency in the use of resources, and for the systems, procedures and practices used to evaluate the effectiveness of operations.

The Data Protection Act 2018 included a change to this structure. Under Section 25 of the 2018 Act, which was commenced with effect from 1 January 2020, the Commissioner, or the Chairperson of the Commission, is now the Accounting Officer for the DPC's expenditure. The DPC now manages its own expenditure directly and DPC funding has been moved from the DJE's Vote into the DPC's own separate Vote (Vote 44) to enable this direct control and accountability.

In preparation for this change of status, the DPC formed an Accounting Officer project team during 2019, with responsibility to prepare and implement the changes that were needed for the DPC to take on this control and accountability directly. These were mainly in the areas of Finance, Governance, Procurement and Corporate Services, and we worked with counterparts from those areas in the Department in defining and implementing the changes. We also engaged with the Department of Public Expenditure and Reform (DPER) and the National Shared Services Office (NSSO) on the changes.

A key output of the project has been the DPC's Corporate Governance Framework which sets out the DPC's governance arrangements, including the establishment of the DPC's new Audit and Risk Committee. The extended and additional activities that our supporting corporate functions must now provide mean that the DPC is now incurring additional pay and non-pay costs from 2020 onwards, so that the DPC can discharge its accounting officer obligations fully.

Phase 2 of the Accounting Officer changes will continue during 2020, mainly linked to the HR and Payroll impact.

Operational Change Programme

During 2019, our operational change programme included several initiatives and improvements that were focused on DPC's internal procedures, processes, systems and management information, for example:

- our ongoing refinement of our internal standard procedures, to take account of our case volumes, our organisational expansion and further clarifications of our powers under the 2018 Act;
- adopting some practical improvements and work-arounds in the EU Internal Markets Information (IMI) system to manage information-sharing with other EDPB data protection supervisory authorities;
- increasing our use of management information and key statistics, and using them to inform organisational changes, process improvements and operational priorities;
- improving the webforms on the DPC website to increase their usability, with further improvements planned for early 2020; and
- reinforcing our existing case management tools to support management information needs and to better serve our growing staff numbers.

All of these initiatives have been key building blocks towards ensuring that the DPC derives the maximum benefits possible from our new Case Management System, on which we will begin phased implementation during 2020.

14

Corporate Affairs



DPC Funding and Staffing

The funding of the DPC by government has increased year-on-year from €1.7 million in 2013 to €15.2 million in 2019 (comprising €8.9 million in pay and €6.3 million in non-pay allocation). The increased funding for 2019 enabled the DPC to continue to grow its staff complement, from 110 at the start of 2019 to 140 at year-end.

The DPC engaged with the Public Appointments Service to recruit staff through the following competitions in 2019:

- Principal Officer — Head of Regulatory Activity
- Principal Officer — Head of Corporate Affairs, Media and Communications
- Assistant Principal Officer — Senior Regulatory Lawyer
- Higher Executive Officer — Legal Researcher
- Higher Executive Officer — Business Systems Analyst

As a result of these recruitment campaigns, the DPC has increased its resources and expertise in key areas. Further recruitment of staff with a wide range of specialisms in 2020 is a priority for the DPC.

Corporate Governance — Code of Practice for the Governance of State Bodies

The DPC is an independent body established under the Data Protection Act 2018, and its statutory governance requirements are set out in that Act. The DPC applies high standards of corporate governance and works to ensure that it follows the requirements set out for all public-sector bodies in the Code of Practice for the Governance of State Bodies (2016), having regard to the DPC's specific statutory governance structure.

As part of the requirements of the Code of Practice, the DPC has a Corporate Governance Assurance Agreement in place with the Department of Justice and Equality (DJE). This Agreement sets out the broad corporate governance framework within which the DPC operates, and defines key roles and responsibilities that underpin the relationship between the DPC and the DJE. As the DPC is independent in the performance of its functions under the provisions of the GDPR and the Data Protection Act 2018, it is not subject to a Performance Delivery Agreement with the Department of Justice and Equality.

In accordance with the Code of Practice for the Governance of State Bodies, the DPC is required to produce an annual Statement on Internal Control. The DPC's Statement covering 2019 is set out at Appendix IV.

From 1 January 2020, the DPC will follow the requirements under the Corporate Governance Standard for the Civil Service (2015) and work began in 2019 in the development of the Data Protection Commission's Corporate Governance Framework.

Risk Management

The Risk Management Policy of the DPC outlines its approach to risk management and the roles and responsibilities of the Senior Management Committee (SMC), heads of areas, as well as managers and staff. The policy also outlines the key aspects of the risk-management process, and how the DPC determines and records risks to the organisation. The DPC implements the procedures outlined in its risk-management policy and maintains a risk register in line with Department of Finance guidelines. This includes carrying out an appropriate assessment of the DPC's principal risks, which involves describing the risk and associated measures or strategies to effectively control and mitigate these risks. The risk register is reviewed by members of the SMC on a regular basis.

Reflecting the key priorities of the DPC, the main risks managed by the office during 2019 were as follows:

- building organisational capacity to meet the enhanced functions of the organisation under the GDPR and national legislation. This included the development of the expertise of the DPC's staff as well as the continued recruitment of new staff with legal, specialist investigatory, and information technology skillset;
- the identification of suitable accommodation to meet the requirements of the DPC as a growing organisation;
- ensuring ongoing effective integration and consolidation of effective and efficient regulatory structures, business processes and functions across the DPC as it implements new and enhanced supervisory functions and responsibilities set out in the GDPR, LED and Data Protection Act 2018; and
- putting in place business processes and policies to directly manage functions such as financial, payroll, HR, ICT, and internal audit in preparation for the DPC transitioning to becoming its own Accounting Officer from 1 January 2020.

Official Languages Act

The DPC's fourth Irish Language Scheme under the Official Languages Act 2003 commenced with effect from 1 November 2017 and remains in effect until October 2020. The DPC continues to provide Irish language services as per our Customer Charter and Irish language information via its website.

Public Sector Human Rights and Equality Duty

The DPC seeks to meet its obligations under Section 42 of the Irish Human Rights and Equality Commission Act 2014 and 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 in fulfilling its mandate to protect the EU fundamental right to data protection.

The Public Sector Equality and Human Rights Duty is referenced in the DPC's Strategy Statement for 2019 and its budget submission for 2020 funding. The Public Sector Equality and Human Rights Duty was reflected upon in the drafting of the public consultation on the DPC's Regulatory Strategy 2020–2025 — Consultation on Target Outcomes.

The DPC has developed and implemented a number of ways in which to communicate with stakeholders, both on an individual basis and in the provision of guidance in an accessible manner. 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. The DPC's commitment to the principles of plain English has been recognised with a 'highly commended' award at the NALA Plain English Awards. The website is designed with regard to com-

pliance with accessibility principles including Website Accessibility Initiative (WAI), Web Content Accessibility Guidelines 2.0 AAA, and ARIA standards. The DPC also operates a helpdesk to facilitate customers.

The DPC has an Accessibility Officer who acts as liaison for the customer and the relevant section of the organisation.

Freedom of Information

The DPC has been partially subject to the Freedom of Information (FOI) Act 2014 since 14 April 2015 in respect of records relating to the general administration of the Office only. Information on making a request under FOI is available on the DPC's website. A disclosure log for all non-personal information requests under the FOI Act is available under our FOI Publication Scheme on the website.

During 2019, the DPC received a total of 46 requests under the FOI Act. Of these, 33 were deemed to be out of scope on the basis that they related to records held by the DPC other than those relating to the general administration of the office. A summary of the FOI requests received by the DPC between during 2019 is included in the table below. No cases were appealed to the Office of the Information Commissioner.

Request by type	Category total	Outcome
Administrative Issues	9	6 granted 1 partially granted 2 dealt with outside of FOI
Matters outside the scope of the Acts	37	33 out of scope 4 withdrawn FOI

In relation to the European Communities (Access to Information on the Environment) Regulation 2007, S.I. No. 133 of 2007, the DPC received no requests in 2019.

Energy Report 2019 — 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. This office will be maintained until a new permanent head office is ready to facilitate the DPC's Dublin-based staff and operations. The office is 828 sq. metres 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 B2.

Portarlinton

The Portarlinton office of the DPC has an area of 444 sq. metres 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 2018 (last validated SEAI figures available) is as follows:

	Electrical	Natural Gas
Dublin		
Fitzwilliam Sq.	88,440Kwh	
Satellite Office	14,687Kwh *	
Portarlinton		
	40,102Kwh	51,308

Overview of Environmental policy / statement for the organisation

The Data Protection Commission 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 run for bin collection services to include compost bin service for Portarlinton & Fitzwilliam Square.
- Reduction of approx. 10% in lighting costs in Fitzwilliam Square following DSE Environmental testing and removal of lights.
- Green Committee 2019 established.

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

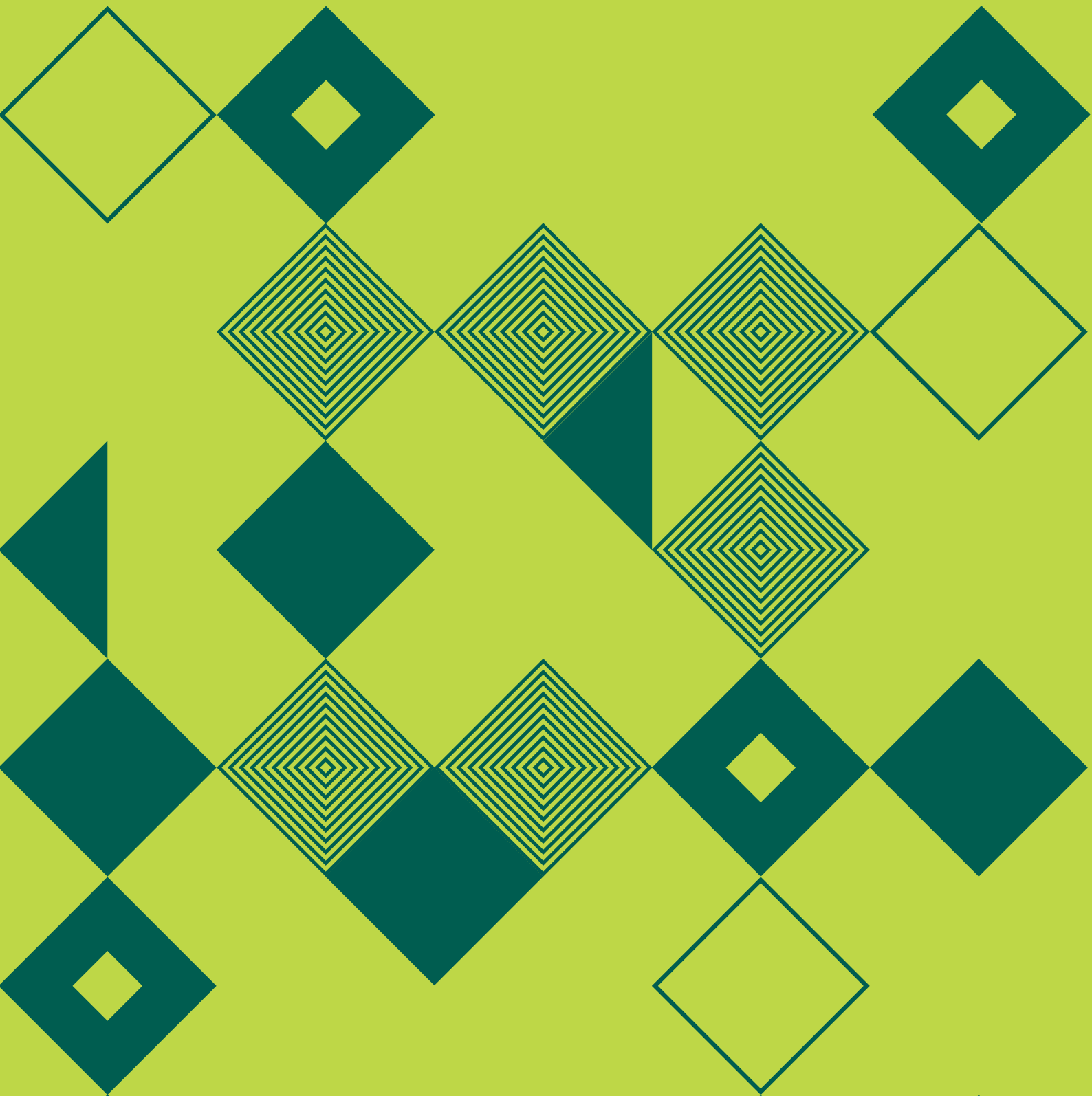
DPC policy is to securely shred all waste paper. Consoles are provided at multiple locations throughout the offices. Shredded paper is recycled.

Sustainable Procurement

DPC procurements and processes are fully compliant with Sustainable Procurement.

Catering contracts stipulate the exclusion of single use plastics.

15 Appendices



Appendix I

Court of Justice of the European Union (CJEU) Case Law

There were a number of significant judgments delivered by the CJEU during 2019 which concerned the interpretation of EU law as it relates to data protection. Key aspects of these judgments, insofar as they relate to issues of data protection, are summarised below.

TK v Asociația de Proprietari bloc M5A-ScaraA (Case C-708/18)

Key issues: video surveillance system in a private property, legal basis, consent, legitimate interest, proportionality. This case was considered under the (now repealed) Data Protection Directive (Directive 95/46/EC).

Facts

This case relates to the lawful basis of a video surveillance system installed in the common areas of an apartment building in Romania. As there had been burglaries and thefts in several apartments and the common areas of the apartment building and the lift had been vandalised on many occasions, the association of co-owners of the building decided to install a video surveillance system in order to monitor who entered and left the building. Romanian law provided for this possibility. Measures which were taken previously, namely the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed. On foot of this, the owner of one apartment in the apartment building sought an injunction order for the removal of this video surveillance system, arguing an infringement of his right to respect for private life and a breach of the Romanian law.

By way of preliminary reference to the CJEU, the Regional Court of Bucharest asked a number of questions referring to the underlying Romanian law and queried as to whether the installation of a video surveillance system in the common areas of a residential building for the purposes of pursuing the legitimate interests of ensuring the safety and protection of individuals and property is proportionate or, alternatively, whether individuals' consent is necessary for such data processing.

Judgment

The CJEU's decision was delivered on 11 December 2019. The CJEU held that the processing of personal data in the context of a video surveillance system must comply first, with the principles relating to data quality (Article 6 of Directive 95/46 (Data Protection Directive)) and, secondly, with one of the criteria to legitimise data processing (as listed in Article 7 of Data Protection Directive). The CJEU noted that Article 7 sets out an exhaustive and restrictive list of six bases pursuant to which the processing of personal data may be regarded as being lawful. One of these bases is pursuant to the legitimate interests of the controller or a third party (Article 7(f)). The CJEU opined that Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements other than those already set out in the Data Protection Directive.

Referring to previous decisions, the CJEU reiterated that, in order to rely on legitimate interests to legitimise data processing, there must be three cumulative conditions satisfied. The first condition is that the legitimate interests pursued by the controller must be present and effective at the time of the data processing. Secondly, there must be the need to process personal data for the purpose of the legitimate interests pursued. This need must be interpreted strictly, in other words, the purpose cannot reasonably be as effectively achieved by other means which are less restrictive of the fundamental rights and freedoms of data subjects. Thirdly, because under Article 7(f)

the rights of a data subject may override the legitimate interests pursued by the controller, this condition necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances. In the context of processing of data from non-public sources, it is essential to assess the seriousness of the infringements of a data subject's rights, taking account of, among the other things, the nature of the personal data at issue such as the potentially sensitive nature of those data, the nature and specific methods of processing of the data such as the number of persons having access to those data and the methods of accessing them, and the data subject's reasonable expectations that his or her personal data will not be processed. The CJEU said that in the present case, those factors must be balanced against the importance of the legitimate interests pursued by the co-owners of the apartment building in relation to the video surveillance system, insofar as this video installation

system seeks to ensure that the property, health and life of those co-owners are protected.

The Court also confirmed that a data subject's consent is not required when processing of personal data occurs pursuant to the legitimate interests of a controller or third party in this context.

The CJEU concluded that provisions of Romanian law which authorise the installation of a video surveillance system in the common areas of a residential building for the purpose of pursuing the legitimate interests of ensuring the safety and protection of individuals and property were not therefore precluded by the Data Protection Directive — as long as the processing by the video surveillance system fulfilled the conditions laid down in Article 7(f). It was for the referring Court to make this assessment.

Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH (Case C-673/17)

Key issues: cookie consent, pre-ticked checkboxes. This case was considered under both the (now repealed) Data Protection Directive (Directive 95/46/EC) and the GDPR, as well as in relation to Directive 2002/58, as amended by Directive 2009/136 (E-Privacy Directive).

Facts

The German Federation of Consumer Organisation (Verbraucherzentrale Bundesverband eV) sought an injunction against an online gaming company, Planet49 GmbH, ordering it to refrain from using a pre-ticked checkbox to gather users' consent to the storage of or access to information in the form of cookies installed on those users' terminal equipment. Planet49 organised a promotional lottery in which participants were required to enter their names and addresses on a web page registration form. The form contained two statements of agreement; one of the statements included a pre-ticked box and the other did not. The pre-ticked statement sought to affirm the participants' agreement to the placement of cookies. The cookies placed on the participants' terminal equipment were linked to names and addresses of the participants provided in the registration form thus the pre-ticked statement was intended to authorise the processing of personal data rather than anonymous data.

The matter came before the German Federal Court which decided to stay the proceedings and to refer a number of questions to the CJEU for a preliminary ruling concerning the requirement in Article 5(3) of the Directive 2002/58, as amended by Directive 2009/136 (E-Privacy Directive)

that users must provide their consent for the storage of, and access to, information in the form of cookies on their terminal equipment.

Judgment

The CJEU's decision was delivered on 1 October 2019. While the preliminary reference was made before the GDPR came into force, the judgment of the CJEU was delivered after the GDPR came into force. The German Federation of Consumer Organisation had also sought an order in the German Courts that Planet49 refrain from **future** action. The CJEU determined first that the questions referred must be answered having regard to both the Data Protection Directive and the GDPR.

On the issue of the validity of the consent to the cookies, the CJEU noted that the E-Privacy Directive defines 'consent' as corresponding to the definition in the Data Protection Directive, however the GDPR had repealed the Data Protection Directive and provided that references to that Directive must be construed as references to the GDPR. The CJEU decided that only active behaviour can fulfil the requirement of consent. First, the CJEU relied on the requirement that consent must be 'unambiguously given' (Article 7(a) of the Data Protection Directive),

reasoning that only active behaviour can dispel ambiguity. Second, the CJEU considered that consent cannot be presumed but must be the result of active behaviour. The CJEU considered that the requirement of active behaviour is also confirmed by the GDPR and noted that the definition of consent is even more stringent in the GDPR than it is in the Data Protection Directive on the basis that the GDPR's recitals expressly require active consent and expressly exclude the possibility of using pre-ticked boxes for the collection of valid consent. Applying this definition of consent, the CJEU held that consent is not valid if cookies are permitted to be placed by way of a pre-checked checkbox which the user must de-select to refuse consent.

The CJEU also considered whether the E-Privacy Directive should be interpreted differently according to whether the information stored or accessed in terminal equipment is personal data or non-personal data. The cookies that Planet49 used were linked to the names and addresses

of the participants in the promotional lottery, and thus, their storage constituted the processing of personal data. The CJEU noted that Article 5(3) E-Privacy Directive applies to information stored in terminal equipment, regardless of whether or not it is personal data.

The CJEU also considered the scope of information that must be provided to users in light of the requirement in Article 5(3) E-Privacy Directive that those users must be provided with clear and comprehensive information prior to providing consent. The Court stated that the user must be in a position to easily determine the consequences of any consent that the user may provide and to understand the functioning of the cookies employed. Additionally, the information that must be provided to users includes the duration of the operation of the cookies and whether or not third parties may have access to the cookies.

G. C. and Others v Commission Nationale de l'Informatique et des Libertés (CNIL) (Déréférencement de données sensibles), (Case C-136/17)

Key issues: right to be forgotten, right to de-referencing, obligations on operators of a search engine, special categories of personal data, information on criminal proceedings. This case was considered under both the (now repealed) Data Protection Directive (Directive 95/46/EC) and the GDPR).

Facts

As an operator of a search engine, Google refused to accede to the requests of four individuals (a local politician; a former public relations officer of the Church of Scientology; a person questioned in the context of a judicial investigation into political funding; and a person previously convicted of sexual offences against children) to de-reference various links to third-party web pages (including press articles) in the list of results displayed by Google in response to searches against their names. Those individuals complained to the French Data Protection Authority (CNIL) which refused to serve formal notices on Google to carry out the de-referencing requested. The case was brought by the four affected individuals before the Conseil d'État (French Administrative Supreme Court) and the Conseil d'État asked the CJEU to clarify the obligations of an operator of a search engine when handling a request for de-referencing under the Data Protection Directive.

Judgment

The CJEU's decision was delivered on 24 September 2019. The CJEU determined firstly that the questions referred

must be answered having regard to both the Data Protection Directive and the GDPR.

The first issue before the CJEU was whether the prohibition and restrictions on processing special categories of personal data, such as those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, data relating to offences, criminal convictions or security measures, also applies to operators of a search engine. The CJEU held that the prohibition and restrictions relating to the processing of special categories of data applies to operators of a search engine in the same way as any other data controller. However, the Court reiterated its decision in *Google Spain*, C-131/12 and noted that the operator of a search engine is only responsible for the reference to a third party web page. Thus, the prohibition and restrictions relating to the processing of special categories of data apply to the operator of a search engine in the context of any request for de-referencing received from a data subject.

In relation to the issue of a request for de-referencing relating to special categories of data, the CJEU stated that, when the operator of a search engine receives such re-

quest, it is in principle required, subject to certain exceptions, to accede to that request. However, the operator may refuse a request for de-referencing if it establishes that the relevant links lead to data which are manifestly made public by the data subject. In any event, the operator must ascertain whether the inclusion of the link to a web page on which special categories of data are published in the list of results displayed following a search of that data subject's name is strictly necessary for protecting the freedom of information of internet users, who may be interested in accessing that web page by means of such a search. The CJEU pointed out that a balancing test between, on the one hand, the data subject's rights to privacy and the protection of personal data and, on the other, the freedom of information of internet users, is necessary based on the specific circumstances of each request and considering the nature of the information in question and its sensitivity in the context of that data subject's private life as well as the interest of the public in having that information. The CJEU noted that the interest of the public may vary according to the role played by the data subject in public life.

In the specific context of a request for de-referencing data relating to criminal proceedings brought against the data subject where that information is now out of date relative to the developments in the proceedings, the CJEU held that, based on the circumstances of the request, the operator of a search engine must assess whether, at the time of the request, the data subject has the right to the information in question no longer being linked with the data subject's name by a list of results displayed following a search of his/her name. Even in this case, the operator must apply a balancing test between a data subject's rights to privacy and the protection of personal data and the freedom of information of internet users. However, whenever the inclusion of the link in question is strictly necessary, the operator of a search engine is required to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means, in particular, that links to web pages containing information in this respect must appear in first place on the list.

Google LLC, successor in law to Google Inc. v Commission Nationale de l'Informatique et des Libertés (CNIL), (Case C-507/17)

Key issues: right to be forgotten, right to de-referencing, obligations of operators of a search engine, removal of the links in all, or only European domain name extensions. This case was considered under both the (now repealed) Data Protection Directive (Directive 95/46/EC) and the GDPR).

Facts

In 2015 the French Data Protection Authority (CNIL) served formal notice on Google to the effect that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person's name, Google must apply that removal to **all** its search engine's domain name extensions. Google refused to comply with that formal notice, but rather only removed the links in question from the results displayed following searches conducted in the domain name extensions corresponding to the versions of its search engine in EU Member States.

In 2016, after finding that Google had failed to comply with that formal notice within the prescribed period, the CNIL imposed a penalty on Google. Google lodged an application with the Conseil d'État (French Administrative Supreme Court) for the annulment of that penalty. By way of a preliminary reference, the Conseil d'État referred certain questions to the CJEU in this context for consideration.

Judgment

The CJEU's decision was delivered on 24 September 2019. The CJEU determined firstly that the questions referred must be answered having regard to both the Data Protection Directive and the GDPR.

On the issue of the territorial scope of the right to de-referencing and reiterating the principles of the right to de-referencing as affirmed previously in the decision *Google Spain* C-131/12, the CJEU considered that the operator of a search engine is required to carry out the de-referencing only on those versions of the search engine corresponding to Member States. In order to ensure a consistent and high level of protection throughout the EU, the CJEU held that the operator must carry out the requested de-referencing not only on the version of the search engine corresponding to the Member State of residence of the person benefitting from that de-referencing but on the versions of the search engine corresponding to all of the EU Member States.

The CJEU also emphasised that although EU law does not require the operator of a search engine to carry out

the requested de-referencing on all the search engine's domain name extensions, it does not prohibit such a practice. Accordingly the Court opined that in the light of the fact, that the interest of the public in accessing information may vary from Member State to Member State (for example, pursuant to derogations available in the Data Protection Directive and the GDPR), a supervisory or judicial authority of a Member State remains competent to

consider a data subject's right to privacy and the protection of personal data concerning him or her and the right to freedom of information in light of national standards of protection for those rights. As such, a supervisory or judicial authority could order, where appropriate, the operator to carry out a de-referencing request in relation to all versions of that search engine.

Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV (Case C-40/17)

Key issues: social plugins, controllership, legitimate interests, consent, duty to inform. This case was considered under the (now repealed) Data Protection Directive (Directive 95/46/EC).

Facts

Fashion ID is an online clothing retailer whose website embedded Facebook's 'Like' social plugin. When an internet user visited Fashion ID's website, that visitor's personal data was transmitted to Facebook as a result of the inclusion of Facebook's "Like" social plug-in on the website. On the basis of the facts contained in the preliminary reference to the CJEU, it appeared that such transmission occurred without that visitor being aware of their data being transmitted to Facebook and irrespective of whether or not he or she was a member of Facebook, or whether he or she clicked on the Facebook 'Like' button.

A German public-service association tasked with safeguarding the interests of consumers (Verbraucherzentrale NRW) criticised Fashion ID for transmitting the personal data of visitors to its website to Facebook on the basis that this transmission occurred without their consent and in breach of the duty to inform visitors of relevant data processing as set out in data protection law.

The association sought an injunction before Düsseldorf Regional Court against Fashion ID to force it to stop the practice of embedding the "Like" social plugin on its website. The Regional Court granted an injunction in favour of the association. Fashion ID subsequently appealed this decision to Düsseldorf Higher Regional Court. The Higher Regional Court then referred a number of questions by way of preliminary reference to the CJEU. These questions centred on whether Fashion ID was a controller of the data collected by the social plugin even if it was unable to influence this data processing; whether it was possible to rely on the lawful basis of legitimate interests to embed the social plugin or whether it was necessary to collect consent of data subjects to the processing; and who should fulfil the duty to inform data subjects of data processing when an operator of the website embeds a third party's social plugin.

Judgment

The CJEU's decision was delivered on 29 July 2019. The CJEU considered firstly whether national legislation may prohibit consumer protection associations from bringing or defending legal proceedings against a person allegedly responsible for an infringement of data protection law. Recalling the underlying objectives of data protection law to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, and, in particular, the right to privacy with respect to the processing of personal data, the CJEU held that the fact that a Member State provides in its national legislation for the possibility for a consumer protection association to commence legal proceedings does not undermine the objectives of that protection, but rather contributes to the realisation of those objectives.

On the issue of controllership of the social plugin, the CJEU held that an operator of a website (such as Fashion ID), which embeds a social plugin of a third party on its website (such as the Facebook "Like" button), causing the browser [in a device] of a visitor to that website to request content from the provider of that plugin and, to that end, to transmit to that provider the personal data of the visitor, can be considered to be a joint controller, with the third party that owns the social plugin. However, the Court considered that liability of the operator of the website is limited to the operation or set of operations involving the processing of personal data in respect of which the operator of the website actually determines the purposes and means i.e. the collection and disclosure by transmission of the data at issue.

On the issue of legitimate interests and social plugins, the CJEU determined that, in a situation in which the operator of a website embeds a social plugin on its website causing the browser of a visitor to that website to request content from the provider of that plugin and, to that end, to

transmit to that provider personal data of the visitor, it is necessary that that operator and that provider each pursue a legitimate interest for the purpose of the respective processing operations in order for those operations to be justified in respect of each of them.

On the issue of consent and provision of information related to social plugins, the CJEU firstly recalled that the duty to obtain the consent of the data subject and the duty to inform are incumbent on that controller which actually determines the purposes and means of the relevant operation or set of operations involving the processing of personal data. The CJEU held that consent must be given prior to the collection and disclosure (in other words the onward transmission) of the data subject's data to third party. In such circumstances, the CJEU said, it is for the operator of the website, rather than for the provider of the social plugin, to obtain that consent. This was

because it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of the social plugin. It is the visiting by the visitor of that website triggers the processing of the personal data. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means. With reference to the duty to inform, this duty is similarly incumbent on the operator of the website but the information that must be provided to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means.

Sergejs Buivids v Datu valsts inspekcija (Case C-345/17)

Key issues: video recording in a police station, publication of video, journalistic exemption. This case was considered under the (now repealed) Data Protection Directive (Directive 95/46/EC).

Facts

Mr Buivids made a video recording in a police station of the Latvian national police while he was making a statement in the context of administrative proceedings which had been brought against him. He later published the video on the Youtube internet site. Following the publication of the video, the National Data Protection Agency of Latvia found that Mr Buivids had infringed data protection law because he had not informed the police officers of the intended purpose of the processing of personal data concerning them and he did not provide any information to the National Data Protection Agency of Latvia as to the purpose of the recording and its publication. Consequently, the National Data Protection Agency requested that Mr Buivids remove the video from YouTube and from other websites.

Mr Buivids brought an action before the Latvian District Administrative Court seeking a declaration that the decision of the National Data Protection Agency was unlawful. Mr Buivids also claimed compensation for the harm he suffered. The Latvian District Administrative Court dismissed the action and subsequently the Latvian Regional Administrative Court dismissed the subsequent appeal. Mr Buivids filed an appeal in the Latvian Supreme Court invoking his right to freedom of expression. By way of preliminary reference to the CJEU, the Latvian Supreme Court asked a number of questions regarding whether the act of filming police officers while carrying out their duties in a police station and the act of publishing this

recorded video on the internet are matters which come within the scope of Data Protection Directive and whether those activities may be regarded as processing of personal data for journalistic purposes.

Judgment

The CJEU's decision was delivered on 14 February 2019. The CJEU held firstly that the once-off act of recording a video using a digital photo camera and publishing the video recording containing personal data on a video website on which users can send, watch and share videos, constitutes processing of those data wholly or partly by automatic means.

The CJEU considered that the recording and publication of the video in question can be regarded as a processing of personal data which falls within the scope of the Data Protection Directive. The Court said that such a video did not constitute a processing operation which concerns public security, defence, State security or the activities of the State in areas of criminal law, as it was the result of activity of a private individual. Moreover, such an activity could not be considered to be purely personal within the context of or household activities because, as a matter of fact, Mr Buivids had published the video in question on a video website on which users can send, watch and share videos, thereby permitting access to the personal data in the video to an indefinite number of people.

On the issue of processing of personal data for journalistic purposes, after recalling the need to balance the right to data protection against freedom of expression, the CJEU reiterated that the right to freedom of expression must be interpreted broadly and that journalistic activities are those which have as their purpose the disclosure of information, opinions or ideas to the public, irrespective of the medium which is used to transmit such information, opinions or ideas. In the circumstances of the case, the Court decided that the fact that Mr Buivids was not a professional journalist did not seem to exclude the possibility that the recording of the video in question and its publication on a video website on which users can send, watch and share videos, could come within the scope of the journalistic exemption. However, the CJEU stated that not all information published on the internet involving personal data can be categorised as journalistic activities. The CJEU indicated that it was for the referring court to determine whether it appeared from the video in question that the sole purpose of the recording and publication of the video was to disclose information, opinion

or ideas to the public particularly taking into account the factual circumstances and whether the video in question was published on an internet site for the purpose of highlighting the alleged police malpractice that Mr Buivids claimed. In order to verify if the journalistic exemption may apply, the referring Court would have to consider this exemption only where it is necessary in order to reconcile two fundamental rights, namely, the right to privacy and the right to freedom of expression, and only in so far as is strictly necessary. The CJEU also held, in relation to the balancing of these two fundamental rights, that the referring Court must take into account, amongst other things, contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, and the manner and circumstances in which the information was obtained and its veracity.

Deutsche Post AG v Hauptzollamt Köln (Case C 496/17)

Key issues: personal data, tax identification number, customs authority authorisation process. This case was considered under both the (now repealed) Data Protection Directive (Directive 95/46/EC) and the GDPR.

Facts

Pursuant to Commission Implementing Regulation (EU) 2015/2447 (which relates to the implementation of customs rules), the German customs authority (the Hauptzollamt) requested that Deutsche Post reply to a self-evaluation questionnaire for the purposes of assessing whether Deutsche Post should have authorised economic operator (AEO) authorisation. (The AEO status allows an entity to benefit from certain simplifications under customs legislation). Under this assessment process, certain information (including tax identification numbers) about owners, shareholders, directors and other officers of Deutsche Post, including those responsible for customs matters, was requested, together with details of the tax offices responsible for the taxation of those persons.

On foot of this request, Deutsche Post brought an action before the Düsseldorf Finance Court, challenging the obligation to send the tax identification numbers of the persons concerned and the details of the tax offices responsible for their taxation to the Hauptzollamt.

The Düsseldorf Finance Court then referred certain matters for a preliminary ruling to the CJEU. The German Court sought to ascertain whether, in the light of Article 8(1) of the Charter and the principle of proportionality, the Hauptzollamt could request personal data, such as

the tax identification numbers of data subjects and the details of the tax offices responsible for the assessment of income tax payable by those persons.

Judgment

The CJEU's decision was delivered on 16 January 2019. The judgment interpreted Regulation 2015/2447 by reference to both the Data Protection Directive and the GDPR. The CJEU firstly recalled that tax data, such as tax identification numbers, constitutes personal data. However, according to the Regulation 2015/2447, the Hauptzollamt, as the national German customs authority, must comply with principles relating to data quality and the legitimacy of data processing whenever it processes personal data in the conduct of its activities.

In this case, the tax identification numbers of natural persons were initially collected by the employer in order to ensure compliance with income tax legislation and, more specifically, to ensure that the employer could fulfil its obligation to deduct and collect income tax at source. In those circumstances, the CJEU found that the subsequent collection of that personal data by a national customs authority (such as the Hauptzollamt) in order to make a decision on an application for the purpose of AEO status in relation to an entity (i.e. in this case, Deutsche Post)

was necessary to comply with Regulation 2015/2447. In particular, a national customs authority must ascertain not only whether an applicant for the purpose of AEO status complies with Regulation 2015/2447, but also whether relevant natural persons within the organisation of that applicant have committed any serious infringement or repeated infringements of that legislation or of the tax rules having regard to the level of their responsibility within the applicant's organisation, irrespective of whether those infringements have any connection to the economic activity of the applicant. To that extent, the CJEU noted that data is collected and therefore processed for specified, explicit and legitimate purposes. Moreover, the CJEU underlined that the data collected by national customs authorities, namely, the tax identification numbers of natural persons listed in Regulation 2015/2447, are adequate, relevant and not excessive in relation to the purposes for which that data is collected.

The CJEU concluded that the data collection by a national customs authority, such as Hauptzollamt, from an applicant for AEO status, of tax identification numbers which are allocated for income tax purposes, which solely relate to the natural persons who are in charge of the applicant or who exercise control over its management and those who are in charge of the applicant's customs matters, and the details of the tax offices responsible for the taxation of all those persons, is permissible only to the extent that such data enables those authorities to obtain information on serious or repeated infringements of customs legislation or of tax rules, or on serious criminal offences committed by those natural persons related to their economic activity.

Appendix II

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 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 data protection authority 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 data protection

authority which involves a claim that an EU Commission decision is incompatible with protection of privacy and fundamental rights and freedoms, the relevant data protection authority must examine that complaint even though the data protection authority cannot itself set aside or disapply that decision. The CJEU ruled that if the data protection authority 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 5 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 European 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 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 2019 before a 5 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 is Judge Thomas von

Danwitz. The Advocate General assigned to the case is Henrik Saugmandsgaard Øe.

At the hearing, the DPC, Mr Schrems and Facebook made oral submissions before the CJEU. The 4 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 European Commission and a number of Member States (Austria, France, Germany, Ireland, Netherlands, and the United Kingdom) 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 Commission Decision underlying the SCCs (SCCs Decision). At the outset, the Advocate General 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 irrespective 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 European 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.

The AG's Opinion is not binding on the CJEU. It is expected that the CJEU will deliver its judgment on the matters referred to it by the Irish High Court at some point in 2020.

Materials relating to the proceedings

The various judgments referred to above, the questions referred to the CJEU, the expert evidence on behalf of the DPC, and the transcripts of the trial before the High Court are available on the DPC's website.

Appendix III

Investigation by the DPC into the processing of personal data by DEASP in relation to the Public Services Card

The DPC's report

On 15 August 2019, the DPC delivered its report in relation to the first part of its investigation into the processing of personal data carried out by the Department of Employment Affairs and Social Protection (DEASP) in connection with the Public Services Card (PSC), to include DEASP's "SAFE 2" registration process.

DEASP published the report on its website⁸ on 17 September 2019, along with its own response.⁹

This first part of the DPC's investigation focused on a defined and limited number of specific issues. In particular, it examined the **legal basis** on which personal data is processed by DEASP in connection with the PSC, and whether the information provided to data subjects in relation to the processing of their personal data in that context satisfied applicable legal requirements in terms of **transparency**. (The DPC's investigation in certain other aspects of processing by DEASP in connection with the PSC is ongoing, as detailed below).

Legal framework for the DPC's investigation

Because the PSC scheme (and the DPC's investigation) pre-dated the coming into effect of the GDPR (the investigation was commenced in October 2017), the DPC's findings were made by reference to particular obligations imposed on controllers under the Data Protection Acts, 1988 and 2003 rather than the GDPR. (This is specifically mandated by the Data Protection Act 2018 which was introduced in 2018 to facilitate the application of particular elements of the GDPR at national level). For completeness, it should be noted that the report also included some (non-binding) material addressing applicable provisions of the GDPR.

⁸ Available at <http://m.welfare.ie/en/pressoffice/Pages/pr170919.aspx>

⁹ Under applicable legislation, it was not open to the DPC to publish the report itself. A statement was issued by the DPC on its own website outlining the scope of the investigation and summarising the report's findings.

Findings

A total of **eight** findings were made in the DPC's report. **Three** of those relate to the **legal basis** issue; the remaining **five** relate to issues around transparency.

Seven of the **eight** findings were adverse to positions advanced by DEASP insofar as the DPC found that there is, or has been, non-compliance with applicable provisions of data protection law.

In summary terms, the DPC found that:

- The processing of certain personal data by DEASP in connection with the issuing of PSCs for the purpose of validating the identity of a person claiming, receiving or presenting for payment of a benefit, has a **legal basis** under applicable data protection law.
- The processing of personal data by DEASP in connection with the issuing of PSCs for the purposes of transactions between individuals and other specified public bodies (i.e. bodies other than DEASP itself) does **not** have a **legal basis** under applicable data protection laws; specifically, such processing contravenes Section 2A of the Data Protection Acts, 1988 and 2003.
- DEASP's **retention** of underlying documents and information provided by persons applying for a PSC on a blanket and indefinite basis contravenes Section 2(1)(c)(iv) of the Data Protection Acts, 1988 and 2003 because such data is being retained for periods longer than is necessary for the purposes for which it was collected.
- In terms of **transparency**, the scheme does not comply with Section 2D of the Data Protection Acts, 1988 and 2003, in that the information provided by DEASP to the public about the processing of their personal data in connection with the issuing of PSCs was not adequate.

(As per the DPC's statement of 16 August 2019 (referenced above), the DPC has determined that PSCs already issued by DEASP will not be treated as invalid and likewise, individuals who access benefits — including free travel — using their PSC will remain free to do so.)

Requirements to address contraventions identified in the report

When delivering its report, the DPC notified DEASP that enforcement action would be deferred to afford the Department an opportunity to identify the measures it would need to implement to bring the PSC scheme into compliance with data protection legislation and to remedy the contraventions identified in the report. The DPC called on DEASP to develop and submit its implementation plan within a period of 6 weeks, and to ensure that the measures necessary to bring the scheme into compliance would be in place no later than 31 December 2019. Separately, however, the DPC called on DEASP to take two specific steps within a period of 21 days:

- (1) Cease all processing of personal data carried out in connection with the issuing of PSCs, where a PSC is issued solely for the purpose of a transaction between a member of the public and a specified public body (i.e. a public body other than DEASP itself).
- (2) Notify all public bodies who require production of a PSC as a pre-condition to entering into a transaction with (or providing a public service to) a member of the public that, going forward, DEASP would not be in a position to issue PSCs to such persons.

DEASP's response to the DPC's findings

DEASP wrote to the DPC on 3 September 2019, noting that, having carefully considered the contents of the report, along with advices received from the Attorney General's office, the Minister was satisfied that, contrary to the position of the DPC, the processing of personal data in connection with the PSC has a strong legal basis. The letter also noted the Minister's position that the information provided to users of the scheme satisfies applicable statutory requirements relating to transparency. Against that backdrop, the letter noted that the Minister considered that it would be inappropriate and potentially unlawful to take the measures required by the DPC. Accordingly, the letter indicated that the Minister had determined that DEASP would continue to operate the PSC scheme and the SAFE 2 identity authentication process, without modification.

Notwithstanding its rejection of the report, and its refusal to formulate and implement measures to bring the scheme into compliance, the letter of 3 September proposed that DEASP and the DPC should nonetheless meet to explore whether measures could be agreed that would obviate the requirement for enforcement proceedings.

A statement was issued by the Minister (along with the Minister for Public Expenditure and Reform) on the same date, in terms that reflected the contents of the letter of 3 September.

The DPC replied to DEASP by letter dated 5 September 2019, explaining the reasons why the DPC considered

that, in light of the rejection of the report's findings, and the Minister's stated determination to continue to operate the PSC scheme, without modification, there could be no basis for engagement between the parties in the manner — or for the purpose — suggested. The letter concluded by noting that, since DEASP was refusing to accept the report's findings, and where it was clear that no implementation plan would be formulated or implemented by DEASP to address the points of non-compliance identified within those findings, the basis on which the DPC had deferred enforcement action no longer applied. Accordingly, the letter indicated that the DPC would now proceed to enforcement.

Following a further exchange of correspondence between the parties in the intervening period, DEASP published its response to the DPC's report on its website on 17 September 2019 together with a statement by the Minister. As well as restating that the Minister and DEASP did not accept the findings contained in the DPC's report, the response and statement reiterated the stated views of the Minister and DEASP to the effect that the PSC has a robust legal basis and so DEASP will continue to issue PSCs for use by a number of public bodies across the public sector. DEASP's response to the report also criticised various aspects of the report, the investigation process which had been followed by the DPC, as well as the process the DPC had called on DEASP to engage with to identify measures to remedy the contraventions of data protection law identified in the report. DEASP also reiterated, in categorical terms, its position that it would continue to operate the PSC and SAFE registration process as it had done to that point.

Enforcement action by the DPC

Ultimately an enforcement notice was issued under Section 10 of the Data Protection Acts 1988 and 2003 on 6 December 2019. That notice, which was directed to the Minister (acting through DEASP), directs the taking of a range of steps in order to remedy the contraventions identified in the DPC's report.

The enforcement notice has since been appealed by the Minister to the Circuit Court. It is expected that the appeal will be heard at some point during 2020.

Continuation of the DPC's investigation into other aspects of processing

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.

Appendix IV

Statement of Internal Controls in Respect of the DPC for the period 1 January 2019 to 31 December 2019

Scope of Responsibility

On behalf of the DPC, I acknowledge responsibility for ensuring that an effective system of internal control is maintained and operated. This responsibility takes account of the requirements of the Code of Practice for the Governance of State Bodies (2016).

Purpose of the System of Internal Control

The system of internal control of the DPC is designed to manage risk to a tolerable level rather than to eliminate it. The system can therefore only provide reasonable and not absolute assurance that assets are safeguarded, transactions are authorised and properly recorded, and that material errors or irregularities are either prevented or detected in a timely way.

The system of internal control, which accords with guidance issued by the Department of Public Expenditure and Reform, has been in place in the office of the DPC for the period of 1st January to 31 December 2019 and up to the date of approval of the financial statements for that period.

Capacity to Handle Risk

The SMC of the DPC acts as the risk committee for the organisation.

The Internal Audit function carries out audits on financial and other controls in the DPC, in line with its annual programme of audits. The DJE Internal Audit Unit carried out an audit at the DPC during 2019.

The DPC's senior management team has developed a risk-management policy that sets out its risk appetite, the risk-management processes in place and the roles and responsibilities of staff in relation to risk. The policy has been issued to all staff who are expected to work within the DPC's risk-management policies, and to alert management of emerging risks and control weaknesses and assume responsibility for risks and controls within their own area of work.

Risk and Control Framework

The DPC has implemented a risk-management system that identifies and reports key risks and the management actions being taken to address and, to the extent possible, mitigate those risks.

A risk register identifies the key risks facing the DPC; these have been identified, evaluated, and graded according to their significance. The register is reviewed and updated by the SMC on a quarterly basis. The outcome of these assessments is used to plan and allocate resources to ensure that risks are managed to an acceptable level. The risk register details the controls and actions needed to mitigate risks and responsibility for operation of controls assigned to specific staff.

I confirm that a control environment containing the following elements is in place:

- Procedures for all key business processes have been documented.
- Financial responsibilities have been assigned at management level with corresponding accountability.
- There is an appropriate budgeting system with an annual budget that is kept under review by senior management.
- There are systems aimed at ensuring the security of the information and communication technology systems. The ICT Division of the DJE provides DPC with ICT services. They have provided an assurance statement outlining the control processes in place in 2019.
- There are systems in place to safeguard the DPC's assets. No grant funding to outside agencies occurs.
- The National Shared Services Office provides Human Resource and Payroll Shared services. The National Shared Services Office provides annual assurances over the services provided. They are audited under the ISAE 3402 certification processes.

Ongoing Monitoring and Review

Formal procedures have been established for monitoring control processes, and control deficiencies are communicated to those responsible for taking corrective action and to management, where relevant, in a timely way. I confirm that the following ongoing monitoring systems are in place:

- Key risks and related controls have been identified and processes have been put in place to monitor the operation of those key controls and report any identified deficiencies.
- An annual audit of financial and other controls is carried out by the DJE's Internal Audit Unit.
- Reporting arrangements have been established at all levels where responsibility for financial management has been assigned.
- There are regular reviews by senior management of periodic and annual performance and financial reports that indicate performance against budgets/forecasts.

Procurement

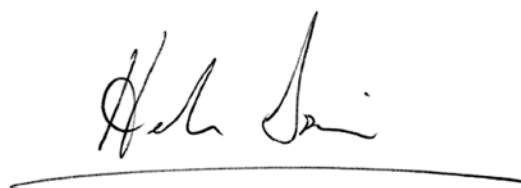
I confirm that the DPC has procedures in place to ensure compliance with current procurement rules and guidelines, and that between 1st January and 31 December 2019 the DPC complied with those procedures.

Review of Effectiveness

I confirm that the DPC has procedures in place to monitor the effectiveness of its risk management and control procedures. The DPC's monitoring and review of the effectiveness of the system of internal financial control is informed by the work of the internal and external auditors, the Audit Committee of the Department of Justice and Equality, and the SMC. The senior management within the DPC is responsible for the development and maintenance of the internal financial control framework.

The DPC's Internal Audit function is carried out by the DJE Internal Audit Unit under the oversight of the Audit Committee of Vote 24 (Justice) for assurance to internal controls and oversight.

The Internal Audit Unit carried out an audit at the DPC during 2019 and reviewed the effectiveness of the internal controls. It should be noted that this extended beyond financial controls and examined ICT controls, management practices and other governance processes. I confirm that the SMC of the DPC kept the effectiveness of internal controls under review between 1st January and 31 December 2019.



Helen Dixon

Commissioner for Data Protection

Appendix V

Report on Protected Disclosures received by the Data Protection Commission in 2019

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 30th 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 2019:

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

- Six 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).

Reference Number	Type	Date Received	Status	Outcome
1/19/1/16	Section 7 (external, to 'prescribed person')	6 November 2019	Open — under examination	
1/19/1/15	Section 7 (external, to 'prescribed person')	3 April 2019	Closed	Closed — complainant did not pursue matter
1/19/1/14	Section 7 (external, to 'prescribed person')	16 March 2019	Open — Being investigated under Article 57(1)(f) of the GDPR	
1/19/1/13	Section 7 (external, to 'prescribed person')	1 March 2019	Closed	Closed — not a protected disclosure — to be handled as a standard DP complaint
1/19/1/12	Section 7 (external, to 'prescribed person')	2 March 2019	Closed	Closed — complainant did not pursue matter.
1/19/1/11	Section 7 (external, to 'prescribed person')	4 February 2019	Closed	Closed — complainant failed to provide evidence of data protection breaches.

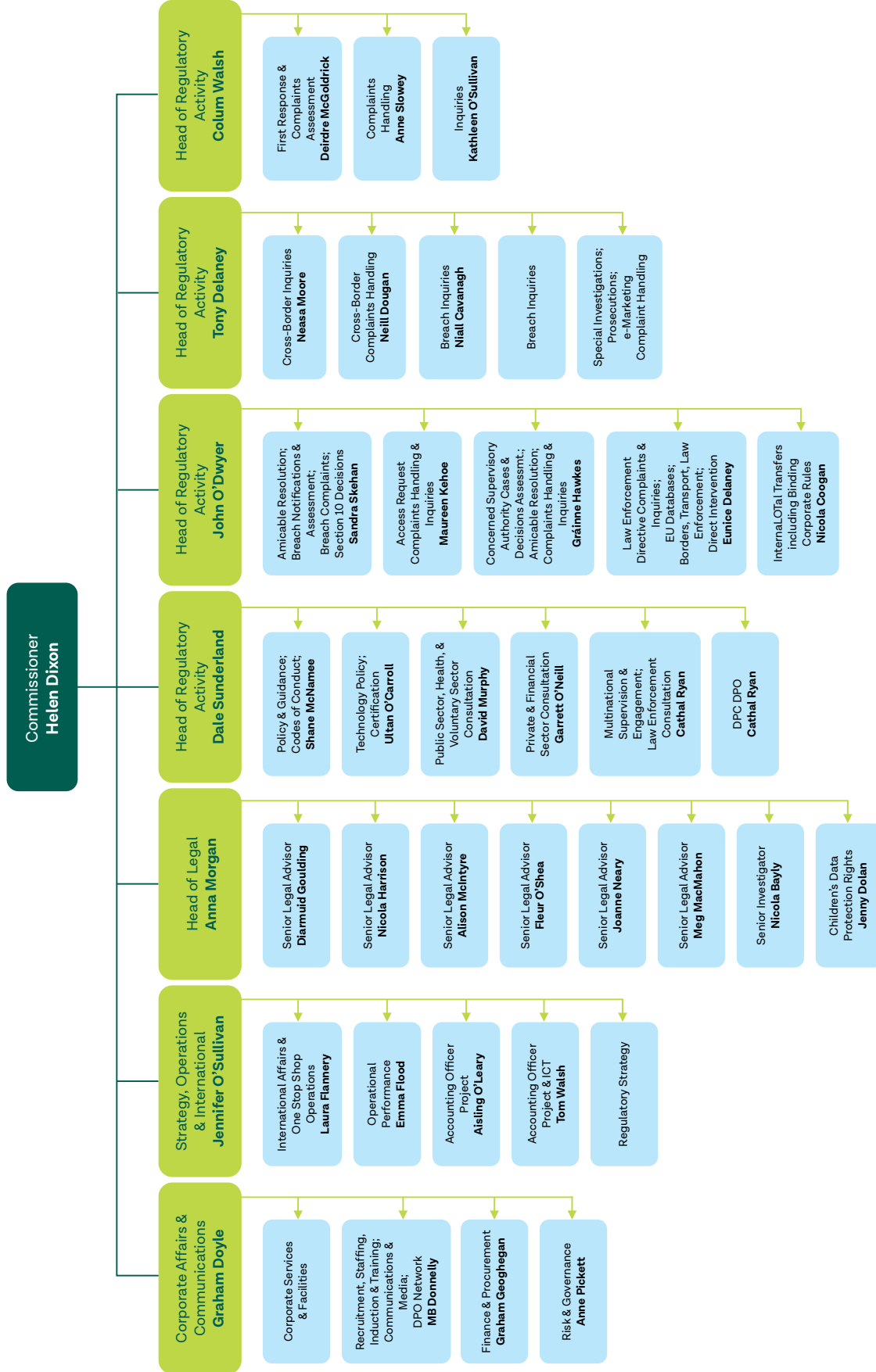
Appendix VI

Financial Statements for the Year 1 January to 31 December 2019

The Account of Receipts and Payments of the Data Protection Commission for the year 1 January to 31 December 2019 is in preparation by the DPC and will be appended to this report following completion of an audit in respect of that year by the Comptroller and Auditor General.

Appendix

Organisation Chart



DPC Senior Team



Ms. Helen Dixon



Mr. Tony Delaney



Mr. Graham Doyle



Ms. Anna Morgan



Mr. John O'Dwyer



Ms. Jennifer O'Sullivan



Mr. Dale Sunderland



Mr. Colum Walsh





Coimisiún
Chosaint Sonraí
Data Protection
Commission

Data Protection Commission,
21 Fitzwilliam Square,
Dublin 2.

www.dataprotection.ie
Email: info@dataprotection.ie
Tel: 0761 104 800



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission