Annual Report

25 May - 31 December 2018

An Coimisiún um Chosaint Sonraí
Data Protection Commission

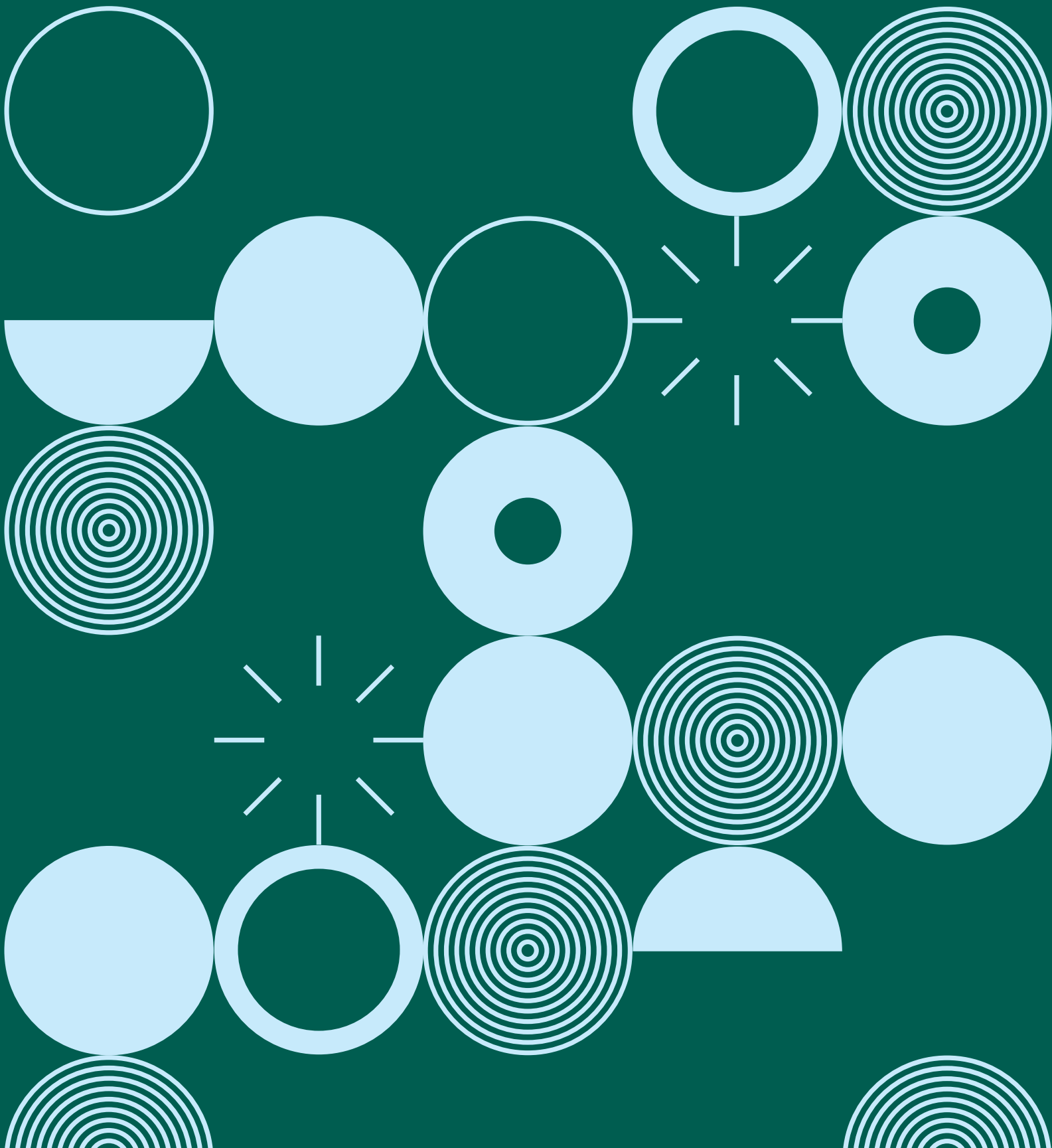


Table of Contents

APPENDICES

Foreword

It is a pleasure to present this first annual report of the new Data Protection Commission (DPC).

The GDPR Effect

The phenomenon that is the General Data Protection Regulation (GDPR) has demonstrated one thing above all else: people's interest in and appetite for understanding and controlling use of their personal data is anything but a reflection of apathy and fatalism. While a series of Eurobarometer surveys* in recent years have catalogued concerns on the part of the public about uses of their data, it is the rise in the number of complaints and queries to data protection authorities across the EU since 25 May 2018 that demonstrates a new level of mobilisation to action on the part of individuals to tackle what they see as misuse or failure to adequately explain what is being done with their data. Pages 18 and 43 of this report details the significant increase in complaints and queries to the Irish DPC.

But the response of industry and the public and voluntary sectors has been just as strong: over 1,000 Data Protection Officers (DPOs) have been appointed by organisations across Ireland and have been notified to the DPC since May. These individuals will play key roles in embedding effective data protection practices in their organisations and driving real improvements in standards of data protection and security. Over 4,000 data breaches have been notified by organisations to the DPC and, while it would be an ideal world if there were fewer, the DPC's experience generally is that most organisations engage with the DPC and accept our guidance around mitigating losses for affected individuals, communicating any high risks to them and learning lessons from the breach to avoid a repeat. In some cases, organisations have provided us with statistical data on the number of access requests, requests for portability and erasure they have received, the systems they have set up to handle such requests, the Data Protection Impact Assessments they have conducted, the training they have instituted for all staff, and, importantly, the sponsorship their data protection programmes is now receiving from their 'C-Suite' executives. Different sectoral groups in Ireland have come together, whether through their DPOs or through representative bodies, to share learning with one another. And if we understand something about the GDPR, it is this: it will be a process of dialogue that lasts many years and the dialogue will need to shift and change with technology, context, learning from evidence (including emerging case law) and evolving societal norms. This will be the route to new context-based solutions and a real understanding of what 'better' looks like.

Engagement and Action

Last year, many organisations and institutions asked the DPC to speak at events, contribute at roundtables or to meet with members, and we facilitated as many of those requests as we could. Each event taught us much about the commitment of leaders in Ireland to get to grips with, and become accountable under, the GDPR. As an office, we continue to roll out as much new guidance as we can because we appreciate the oft-needed clarification arising from the principles-based nature of the law. While we are still in the stage of having to bust some myths and misunderstandings that have built up around GDPR (the inability of a hairdresser to provide details of hair dye to a customer because of GDPR seems to be a firm favourite!)**, as an office, we feel very optimistic about the improvements we will see in Ireland in personal-data-handling practices over the next few years. When we announced recently that we would roll out supports for a DPO network in Ireland in Q2 of 2019, the response was immediate in terms of a desire on the part of organisations to maintain an active and engaged dialogue with peers and the data protection authority.

* http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_en.pdf

** https://www.rte.ie/radio1/liveline/programmes/2018/1107/1009323-liveline-wednesday-7-november-2018/

While we are optimistic, there are of course many issues that persist on the ground. The DPC has significant resources assigned to investigations of large-scale data processing by the state in terms of our examination of the Public Services Card (PSC); its registration system and the mandatory requirement to produce the PSC to the exclusion of any other form of identity for certain non-social welfare-state services; the surveillance of public spaces by state agencies; and the security of data-processing by Tusla, the Child and Family Agency.

Equally, Ireland is home to many multinational internet and tech companies, and in 2018 the DPC opened inquiries into data-processing activities of Facebook, Apple, Twitter, LinkedIn, WhatsApp and Instagram, looking at issues ranging from large-scale data breaches to legal bases for processing to transparent presentation to users. All these inquiries should reach the decision and adjudication stage later this year, and it's our intention that the analysis and conclusions in the context of those inquiries will provide precedents for better implementation of the principles of the GDPR across key aspects of internet and ad tech services. There are undoubtedly areas of risk to be examined in sectors beyond the free internet services but initial complaints and breaches have focused the DPC in this area and warrant attention in light of the hundreds of millions of users implicated.

EU Cooperation

Our fellow EU regulators, alongside whom we sit on the European Data Protection Board (EDPB), follow the activities and results of the Irish DPC closely, given that a significant number of people in every EU member state are potentially impacted by processing activities of the internet companies located in Ireland. EDPB activity is intense, with monthly plenary meetings and a new system of online data sharing in relation to cross-border processing cases rolled out between the authorities. The DPC has led on the development of EDPB guidance on arrangements for Codes of Conduct under the GDPR and these should be approved and published by the EDPB in Q1 of 2019. The DPC looks forward to industry embracing Codes of Conduct and raising the bar in individual sectors in terms of standards of data protection and transparency. Codes of Conduct are important because they will more comprehensively reflect the context and reality of data-processing activities in a given sector and provide clarity to those who sign up to the standards that need to be attained in addition to external monitoring by an independent body. It is clarity of standards that will drive real results.

Children

In this context, the DPC has launched a large-scale consultation around the processing of children's data. The consultation is open to submissions from any party until 1 March 2019 (Edit: date has been extended to 5 April 2019), and a special stream of the consultation is rolling out during Q1 of 2019 in schools and Youthreach centres to gather the perspectives of children aged 8 to 16 on the issues. The consultation will look at the following:

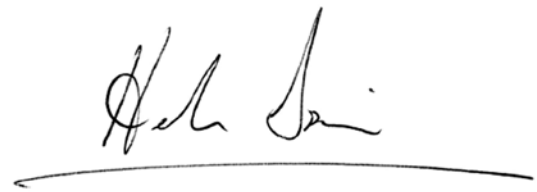
- how, when and in what contexts children may exercise their own rights independently of their parents or guardians;
- views on the age at which children should be able to sign up to free apps in their own right;
- how age should be verified by service providers; and
- how parental or guardian approval should be sought and verified if required.

A best-practice guidance note reflecting the results of the consultation will be produced by the DPC, and ultimately we will look to industry sectors to adopt Codes of Conduct upholding these standards.

Big Year Ahead

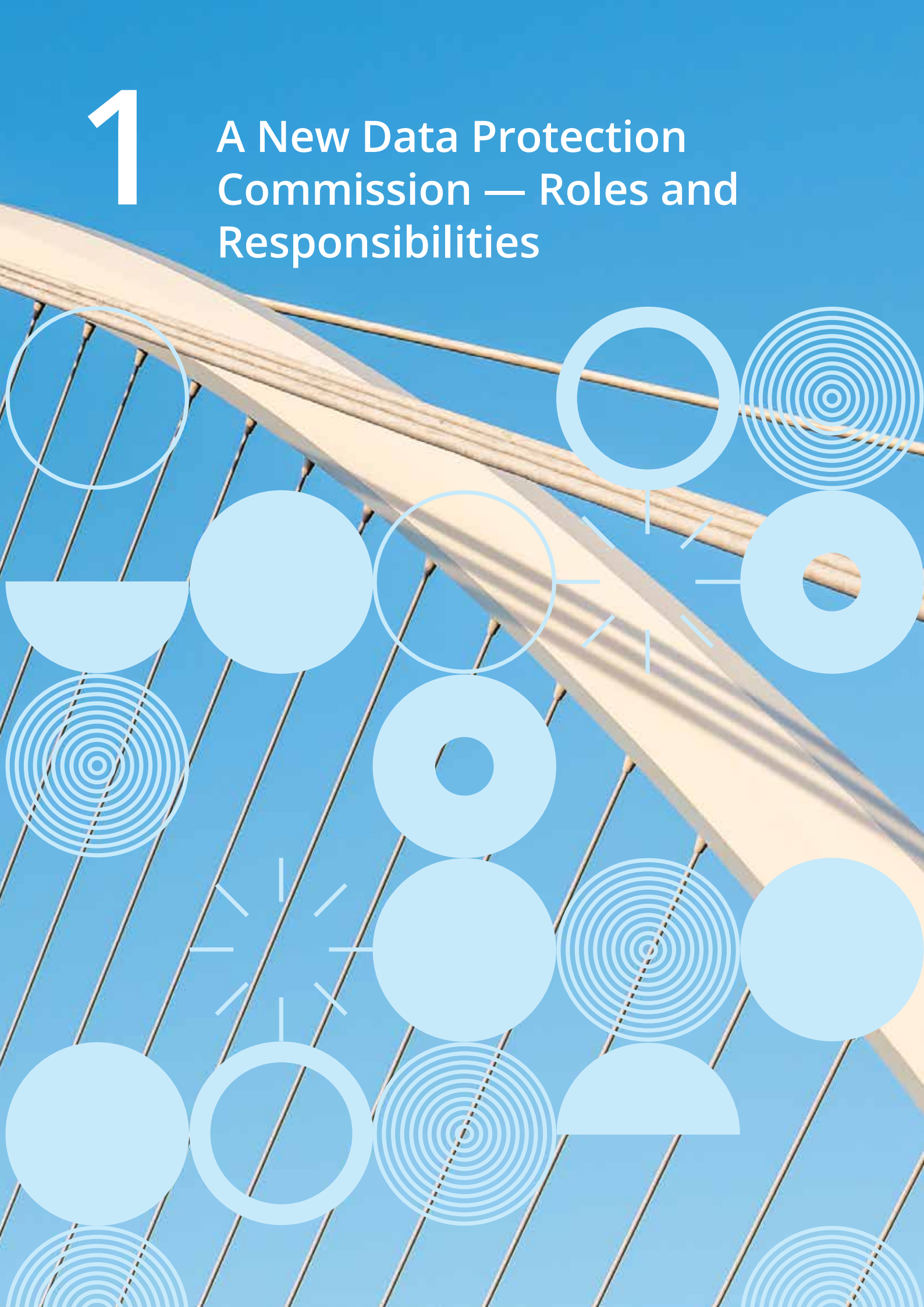
Much new salient case law is expected from the Court of Justice of the European Union (CJEU) in 2019. The Advocate General opinion and CJEU ruling in the Planet49 case are eagerly awaited to provide guidance on cookie-based transparency and consent. Equally, it is anticipated that the High Court reference case from Ireland on the validity of Standard Contractual Clauses will also be heard and decided this year. Further enforcement actions from all data protection authorities in the EU will also conclude, providing additional insight into interpretation of the principles of the GDPR in different scenarios.

The Irish DPC has been in expansion mode for the past four years and we are not stopping now. Following a major recruitment campaign in 2018, 30 new staff had joined the DPC by the end of December, with a further 20 coming on board in January 2019, so that the DPC has grown to 135 staff. We will recruit an additional 30 staff this year in order to meet the demands of the tasks assigned under the GDPR and to deliver public value in what is an area of critical importance to society. In order to underpin delivery of our mission, in early Q2 of 2019 the DPC will launch a consultation on a five-year regulatory strategy, allowing broad stakeholder input into how we deploy our resources and make regulatory choices to deliver the best outcomes, including behaviours that don't just deliver cosmetic compliance but also meet consumer expectations. It's going to be a big first calendar year of the GDPR — let's keep in touch.



Helen Dixon
Commissioner for Data Protection

1 A New Data Protection Commission — Roles and Responsibilities



May 25, 2018 was an historic day across the EU with the application of the General Data Protection Regulation (GDPR), and in Ireland with the commencement of the Data Protection Act 2018 and the establishment of a new Data Protection Commission. This new legal framework has brought about a transformative change in data protection regulation, strengthening the responsibilities of organisations when processing personal data and enhancing the data protection rights of individuals.

Since 25 May 2018, in accordance with this new legislation, the DPC is no longer a data protection authority with a purely national focus; it has become a supervisory authority with an EU-wide remit, responsible for protecting the data privacy rights of millions of individuals across the EU.

This is the first annual report of the new DPC. It has been prepared in accordance with Section 24 of the Data Protection Act 2018 and covers the period from 25 May to 31 December 2018.

Functions of the new 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 data controllers and processors;
- 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 Senior Management Committee

The DPC's Senior Management Committee (SMC) comprises the Commissioner for Data Protection and the five Deputy Commissioners. The Commissioner and the

other 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 Dale Sunderland (Deputy Commissioner — Head of Technology Multinationals Supervision & Investigations; Prior Consultation & Engagement);
- Ms Jennifer O'Sullivan (Deputy Commissioner — Head of Strategy, Operations & International);
- Mr John O'Dwyer (Deputy Commissioner — Head of Breaches, Complaints, Investigations & Transfers); and
- Ms Marita Kinsella (Deputy Commissioner — Head of Corporate Affairs & First Response).

Funding and Administration

That the data protection authority in each EU member state is independent in the performance of its functions is fundamental to the GDPR. In addition, under the GPDR the Irish Government, similar to all EU member state governments, is required to ensure that the DPC has the human, technical and financial resources, as well as the premises and infrastructure necessary to effectively perform its functions.

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 recent years, through its ongoing support for the expansion of the DPC, the Irish Government has continued to demonstrate its commitment to upholding data protection rights and to the central role of the DPC in data protection regulation at EU level. Government funding of the DPC has increased significantly in recent years from €1.7 million in 2013 to €11.7 million in 2018 (comprising €7.3 million pay allocation and €4.4 million non-pay allocation). The DPC very much welcomes the government's continuing commitment to resourcing the needs of the DPC in performing its expanding role as a leading EU supervisory authority.

The allocation of funding to the DPC under Budget 2018 was done on a full-year basis. In accordance with Part 4 of the Data Protection Act 2018, the DPC's 2018 allocation transferred to the new Data Protection Commission upon its establishment on 25 May 2018.

For the year 2018, the DPC prepared two financial statements, the first covering the period from 1 January to 24 May 2018 in respect of the office of the Data Protection Commissioner, and the second covering the period from 25 May to 31 December 2018 in respect of the newly-established Data Protection Commission. The Financial Statement for the DPC in respect of the period covered by this report will be appended following the conduct of an audit by the Comptroller and Auditor General.

The DPC's Strategic Objectives for 2018

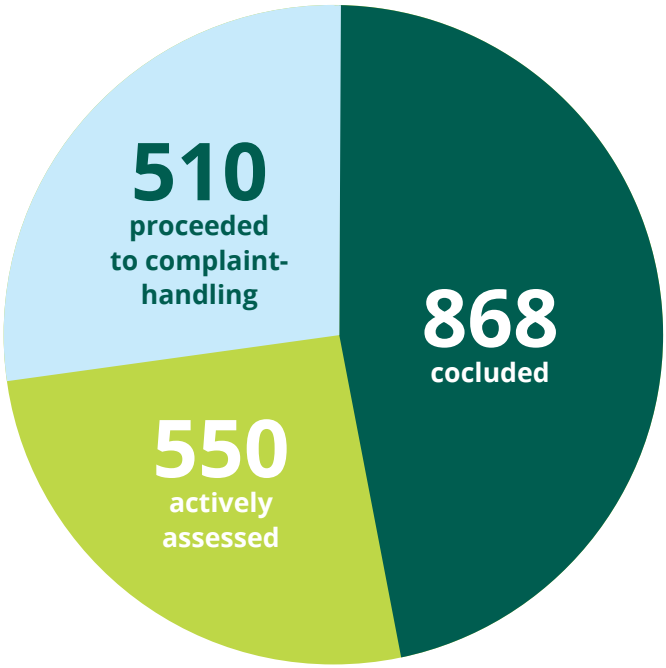
Acknowledging that the period from 2017 to 2018 would be a time of immense transformation, both for the DPC itself as a regulatory body and also for its regulatory environment in light of the GDPR, the DPC put in place a Statement of Strategy. The Statement of Strategy set out strategic objectives that were specific to the revolutionary change ongoing in the DPC. As planned, a review of this Statement of Strategy was carried out towards the end of 2018, to evaluate the DPC's progress against its strategic objectives and to assess the continuing relevance of its mission, vision and values.

In accordance with the DPC's Statement of Strategy 2017-2018, the main goals for the period covered by this report were as follows:

1. **Further develop the capacity and capabilities of the DPC to reflect our enhanced role under the new GDPR, Law Enforcement Directive and e-Privacy Regulation regime by:**
    - proactively engaging with government to ensure we have the required regulatory powers, as well as financial and other resources, including appropriate accommodation and staff, to enable the DPC to perform its role efficiently and effectively;
    - further strengthening our capacity and expertise through the development and upskilling of staff, as well as the targeted recruitment of staff with specialist skills; and
    - concluding work on the redevelopment of our processes, systems (including our ICT capabilities) and structures, to ensure our continued effectiveness under the new data protection regime.
2. **Collaborate with EU and international data protection authority (DPA) counterparts, and regulatory bodies in other sectors by:**
    - developing strong and effective relationships with other EU counterparts and regulatory bodies, including via the European Data Protection Supervisor's Digital Clearing House Initiative — bringing together Competition, Consumer, and Data Protection Regulators;
    - engaging proactively and contributing at EU level through the Article 29 Working Party (comprising the EU's DPAs) to the development of a harmonised interpretation of the new laws, preparation of GDPR guidance, and the evolution of the EU procedural framework for the new laws, in advance of 25 May 2018;
    - promoting bilateral cooperation and information-sharing by hosting delegations from EU and International Data Protection Authorities and authorising their participation in DPC audits and inspections;
    - participating effectively and constructively in the new European Data Protection Board (EDPB), with the objective of contributing to the consistent and proper implementation of the new laws, as well as the development of common positions and responses to pan-EU data privacy developments; and
    - continuing to foster close relationships with International DPAs through forums such as the Global Privacy Enforcement Network and the International Conference of Data Protection and Privacy Commissioners.
3. **Driving better data protection awareness and compliance through strategic consultation by:**
    - proactively targeting and engaging with public and private-sector organisations, particularly in areas of highest risk and large-scale systemic data processing;
    - providing clear, high-quality and timely guidance to data controllers and processors, including by maximising the use of social media and online communication channels; and
    - delivering a high-volume outreach programme to national, EU and international stakeholders as keynote speakers at conferences and participation in panel and workshop events.
4. **Ensure effective oversight and enforcement by:**
    - engaging effectively with stakeholders, our EU counterparts and other regulatory bodies to identify key areas of bad practice and serious non-compliance, which might require enforcement measures;
    - pursuing regulatory action, including the imposition of sanctions, in a lawful, fair, proportionate and effective manner, which accords with the harmonised EU approach, with the overall objective of driving better compliance and accountability by organisations in upholding their obligations to data subjects; and
    - driving improved compliance with data protection obligations through investigations and audits targeting the high-risk and large-scale processing of personal data.

2 Review of 25 May — 31 December 2018

- Total Complaints received was **2,864**, with the largest single category being "Access Rights".
- **1,928** GDPR complaints and **936** complaints under the Data Protection Acts 1988 and 2003.

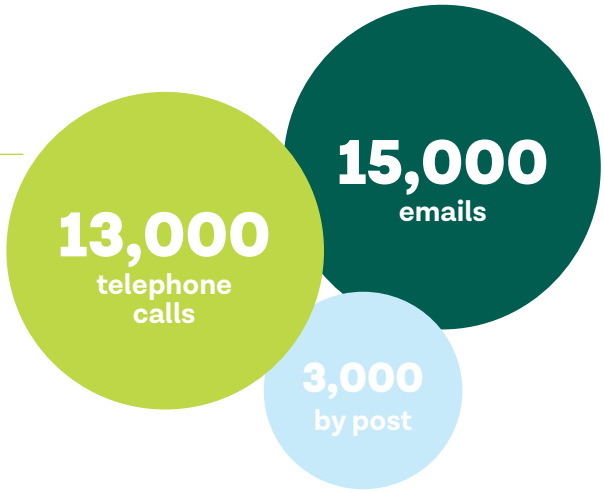


- Of the 1,928 GDPR-related complaints received, **550** complaints were actively being assessed; **510** complaints had proceeded to complaint-handling; and **868** had been concluded.
- **612** complaints were also concluded under the Data Protection Acts 1988 and 2003.

- While the majority of complaints continued to be amicably resolved, the DPC issued a total of **18** formal decisions. Of these, **13** upheld the complaint and **5** rejected the complaint.
- **32** new complaints were investigated under S.I. 336 of 2011 in respect of various forms of electronic direct marketing: **18** related to email marketing; **11** related to SMS (text message) marketing; and **3** related to telephone marketing.
- A number of these investigations concluded with successful District Court prosecutions by the DPC. Prosecutions were concluded during this period against five entities in respect of a total of **30** offences under the E-Privacy Regulations.

- **136** 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.
- **48** data-breach complaints were handled by the DPC from affected data subjects.
- **3,542** valid data security breaches were recorded, with the largest single category being "Unauthorised Disclosures".
- **38** of these data breaches related to **11** multinational technology companies.

- The Information and Assessment Unit received almost **31,000** contacts comprising approximately **15,000** emails, **13,000** telephone calls and **3,000** items of correspondence via post.
- The Special Investigations Unit (SIU) opened **31** own-volition inquiries under the Data Protection Act 2018 into the 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 SIU continued its work in relation to the special investigation into the Public Services Card of the Department of Employment Affairs and Social Protection.



- **15** statutory inquiries (investigations) were opened in relation to multinational technology companies compliance with the GDPR.
- In relation to the multinational technology sector, the DPC received **16** requests – formal and voluntary – for mutual assistance from other EU data protection authorities.
- In late 2018, the DPC established an advanced technology evaluation and assessment unit (the Technology Leadership Unit – TLU) with the objective of supporting and maximising the effectiveness of the DPC's supervision and enforcement teams in assessing risks relating to the dynamics of complex systems and technology.
- The number of general consultation queries received was **958** (these figures do not include consultations with multinational technology companies).

- During the period 25 May – 31 December 2018 there were developments in the DPC's High Court litigation seeking a reference to the CJEU on the validity of SCCs as a transfer mechanism in respect of EU — US data transfers. In July, the Supreme Court granted leave to Facebook allowing it to bring its appeal against the judgments delivered by the High Court in favour of the DPC on 3 October 2017 (as revised on 12 April 2018). During late 2018, there were several procedural hearings in the Supreme Court in preparation for the hearing of the appeal proper, which took place in January 2019. At the time of going to print there is no indication as to when the Supreme Court judgment will be delivered. The High Court's reference to the CJEU remains valid and is pending before the CJEU.
- The DPC continued to act, or commenced acting, as lead reviewer in relation to **11** Binding Corporate Rules (BCRs) applications.
- DPC staff spoke and presented at events on over **110** occasions, including conferences, seminars, and presentations to individual organisations from a broad range of sectors.
- In Q4 of 2018, there was a major redesign and relaunch of the main DPC website, **www.dataprotection.ie**. The new website offers extensive guidance and resources for the public as well as for data controllers and data processors that has either been updated or newly developed for the DPC's new statutory frameworks. Complaints, data-breach notifications and general queries can now be submitted to the DPC through its online webforms.
- Between 25 May and 31 December 2018, the DPC expanded its social media activities across Twitter and LinkedIn, and at year-end had a combined followership of approximately **10,000**, and an organic monthly reach in the hundreds of thousands.
- The first stream of a public consultation on the processing of children's personal data and the rights of children as data subjects under the GDPR was launched on 19 December 2018, with a closing date of 1 March 2019. This stream aimed to engage adult stakeholders, including parents, educators, organisations that represent children's rights, child-protection organisations, representative bodies for parents and educators, and organisations that collect and process children's data.
- In late 2018, the DPC commenced a significant project to develop a new five-year DPC regulatory strategy. This will include extensive external consultation during 2019, which will be central to the analysis, deliberation and conclusions on our enduring strategy.
- The DPC received **900** Data Protection Officer notifications.
- A new Operational Performance Unit was established in the latter part of 2018 to drive the DPC's ongoing programme of change.

3 Complaints

Since the application of the GDPR, the DPC has seen a significant increase in the number of complaints received. Between 25 May and 31 December 2018, 2,864 complaints were received by the DPC.

The DPC received complaints under two substantive parallel legal frameworks during this period:

- Complaints and potential infringements that related to, or occurred, before 25 May 2018, must be handled by the DPC under the framework of the Data Protection Acts 1988 and 2003; and
- In addition and separately, complaints received by the DPC relating to the period from 25 May 2018 must be dealt with by the DPC under the new EU legal framework of the GDPR and Law Enforcement Directive and the provisions of the Data Protection Act 2018 which give further effect to/transposes those laws.

Complaint-handling under the GDPR, the Data Protection Act 2018 and the Law Enforcement Directive

The term "complaint" has a very specific meaning under the GDPR (as well as the Law Enforcement Directive) 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:

- An individual can complain to the DPC but for it to constitute a "complaint" within the meaning of the law, it must relate to the processing or his or her own personal data and it must also indicate that the individual believes that there has been an infringement of the GDPR, the Law Enforcement Directive or the Data Protection Act 2018 by the controller or processor about which the complaint is made.
- It is also possible for a complaint to be made by one individual on behalf of another where there is a legal entitlement, or legal authorisation, to do so on their behalf; and
- The GDPR, Law Enforcement Directive and the Data Protection Act 2018 now specifically recognise that certain types of not-for-profit bodies that have data protection or privacy objectives can lodge a complaint on behalf of an individual who has authorised them to do so. Again, to constitute a complaint within the meaning of the law, it must relate to the personal data of the person on whose behalf the complaint is made and it must also relate to an alleged infringement of the GDPR, the Law Enforcement Directive or the Data Protection Act 2018.

Throughout the period when the complaint-handling process is ongoing, the DPC has an obligation to provide the complainant with updates in relation to the progression of their complaint and ultimately to inform the complainant of the outcome of the complaint. The DPC issues updates to complainants every three months in accordance with its obligations.

In the lead-up to the application of the GDPR, the DPC's awareness campaigns together with the broad media coverage of the changes brought in by GDPR and its impacts, led to much greater public consciousness of data protection issues and rights. This was reflected in the increase in complaints received by the DPC after 25 May 2018 relating to the processing of personal data that took place under the previous legislative regime.

Of the 2,864 complaints received by the DPC between 25 May and 31 December 2018, 1,928 were GDPR complaints, while 936 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 25 May and 31 December 2018, though in proportion to overall complaints it is dropping. Complaints relating to "Unfair Processing of Data" and "Disclosure" were also once again received in high volumes.

In the period between 25 May and 31 December 2018, the Commissioner issued 18 decisions under the Data Protection Acts 1988 & 2003. Of these, 13 fully upheld the complaint and 5 rejected the complaint.

Electronic Direct-Marketing Complaints

During the period under review, a total of 32 new complaints were investigated under S.I. No. 336 of 2011 in respect of various forms of electronic direct marketing.

Of the 32 complaints investigated, 18 related to email marketing, 11 related to SMS (text message) marketing and three related to telephone marketing.

We concluded 41 electronic marketing complaint investigations in the period under review.

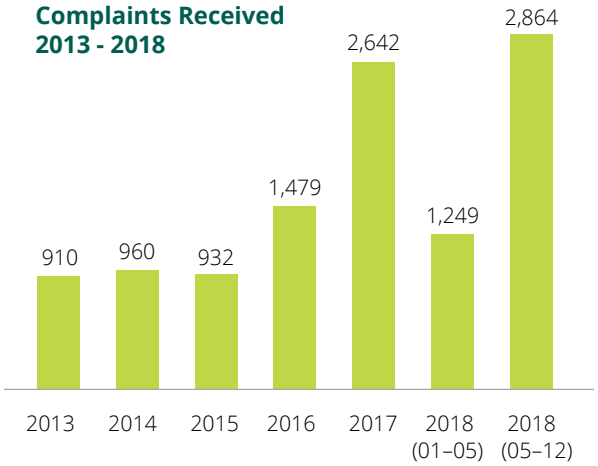
GDPR 2018 (25 May — 31 Dec 2018) — Breakdown by complaint type

	Percentages	Totals
Access Rights	30%	582
Multinational Complaints — Others	22%	396
Unfair Processing of Data	15%	285
Disclosure	11%	217
Electronic Direct Marketing	6%	111
Fair Obtaining	5%	100
Use of CCTV Footage	2%	35
Failure to secure data	2%	33
Internet Search Result Delisting	2%	31
Right of Rectification	2%	30
Retention	1%	28
Multinational Complaints — Access Rights	2%	25
Excessive Data	<1%	16
Accuracy	<1%	16
Unauthorised Access	<1%	9
Specified Purpose	<1%	6
Postal Direct Marketing	<1%	4
Biometrics	<1%	4
TOTALS	**100%**	**1,928**

Data Protection Acts 1988 and 2003 (25 May to 31 Dec 2018) — Breakdown by complaint type

	Percentages	Totals
Access Rights	39%	365
Unfair Processing of Data	19%	178
Disclosure	15%	138
Fair obtaining	8%	74
Electronic Direct Marketing	4%	36
Use of CCTV Footage	3%	29
Failure to secure data	2%	19
Retention	2%	15
Internet Search Result Delisting	2%	14
Excessive Data	2%	13
Specified Purpose	2%	12
Right of Rectification	1%	10
Accuracy	1%	9
Unauthorised Access	<1%	9
Multinational Complaints — Others	<1%	7
Multinational Complaints — Access Rights	<1%	5
Postal Direct Marketing	<1%	2
Biometrics	<1%	1
TOTALS	**100%**	**936**

The two tables above illustrate the complaint types received by the DPC under the GDPR (Table 1) and the Data Protection Acts 1988-2003 (Table 2).



Complaint Case Studies

CASE STUDY 1
Transmission of data by a Government Department via WhatsApp
(Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint against the Department of Foreign Affairs and Trade (the DFAT), alleging that the mission in Cairo, Egypt, had shared the complainant's personal data with a third party (his employer) without his knowledge or consent, and that it had failed to keep the complainant's personal data safe and secure, having transmitted it via WhatsApp to his employer. This related to processing of the complainant's personal data contained in a short-term visa application that the complainant had submitted in order to sit an exam in Ireland.

During our investigation, the DFAT informed us that it was standard practice in processing visa applications to check for accuracy, completeness and the validity of supporting documents. According to DFAT, a suspicion had arisen as to the veracity of a supporting document submitted by the complainant, which had purportedly been signed by his employer. In order to verify its validity, a staff member in the Cairo mission had contacted the employer (an official of an Egyptian government agency, whose name and signature appeared on the document) by telephone as he was best placed to verify the authenticity of the document. The employer confirmed that he would need to see the document to verify it, but that as he did not have an official email address, the only way to receive it was via WhatsApp. The DFAT informed us that prior to sending the data via WhatsApp it had carried out a local risk assessment, including looking at the security/encryption associated with WhatsApp. It had concluded that in light of the end-to-end encryption on WhatsApp, this was the most secure means of transmission available, given the urgency of the visa application, as outlined by the complainant in his application. In this context, DFAT informed us that many government officials and civil servants in Egypt do not have access to official email accounts/systems and often use services like Gmail, Hotmail, WhatsApp and Viber to carry out official business. In this case, the government official in question had confirmed that this was the only method of communication available to him.

The documents had been sent by using the mobile phone of the only staff member of the Cairo mission with WhatsApp and had been deleted from the device immediately after being sent. Ultimately, the official informed the Cairo mission that the documents were fraudulent and the visa application was denied.

During our investigation, the complainant informed us that he was seeking €3,000 in compensation from the DFAT, as the lost cost of sitting the exam in Ireland. Upon the DPC informing the complainant that it did not have the power to award compensation, the complainant requested a formal decision from the DPC.

In considering whether a contravention of the Acts had occurred when the complainant's personal data was sent by DFAT, via WhatsApp to the official in question, the DPC sought to establish the facts in relation to, first, whether the transmission in question was necessary, and, second, whether it was secure, including whether there were more secure methods available to DFAT to transmit the data. On the first issue, the DPC was satisfied that it was necessary for the DFAT to share the complainant's personal data with the official who, in the application for the short-term visa, was stated to be his employer and who, according to the application documents, had purportedly signed certain supporting documents. We noted in this regard that the relevant privacy policy (for the Irish Naturalisation and Immigration Services) explicitly states that burden of proof in a visa application is on the applicant and that the visa officer may verify any evidence submitted in support of an application. The policy also states that any information provided in an application form can be disclosed to, among others, foreign governments and other bodies for immigration purposes.

The DPC was satisfied that given the lack of any other secure means to contact the official in question, the transmission via WhatsApp was necessary to process the

personal data for the purpose provided (visa eligibility) and that the complainant was on notice that supporting documentation could be shared with third parties to verify authenticity. The DPC also took account of the fact that the local risk assessment carried out by DFAT had established that, in the circumstances, sending the personal data via WhatsApp was the most secure means of transmission. Accordingly the DPC found that DFAT had complied with the Acts.

This was an exceptional case arising from the particular on-the-ground circumstances of the country in question. Here, transmission of information for official purposes via WhatsApp was in fact the most secure method available and the complainant's employer, while a government official, had no access to an official communications system through which the personal data could have been transmitted. In this case, the key data protection principles of necessity and proportionality, applied against the unique context of the processing in question, resulted in the DPC reaching a finding of compliance with the Acts. Such a finding would likely not have prevailed had the complaint arisen in an equivalent case where other official communication channels had been available to transmit the personal data contained in the supporting documents.

CASE STUDY 2
Provision of CCTV footage by a bar to an employer
(Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint against a city-centre bar, alleging that it had disclosed the complainant's personal data, contained in CCTV footage, to his employer without his knowledge or consent and that it did not have proper CCTV signage notifying the public that CCTV recording was taking place.

During our investigation, we established that a workplace social event had been hosted by an employer organisation in the bar on the night in question. The complainant was an employee of that organisation and had attended the workplace social event in the bar. An incident involving the complainant and another employee had taken place in the context of that workplace social event and there was an allegation of a serious assault having occurred. An Garda Síochána had been called to the premises on the night in question and the incident had been reported for a second time by the then manager and headwaiter to the local Garda station the following day. We established that the employer organisation had become aware of the incident and had contacted the bar to verify the reports it had received. Ultimately the bar manager had allowed an HR officer from the employer organisation to view the CCTV footage on the premises. The HR officer, upon viewing the CCTV footage, considered it a serious incident and requested a copy of the footage so that the employer organisation could address the issue with the complainant. The bar manager allowed the HR officer to take a copy of the footage on their mobile phone as the footage download facility was not working.

The DPC considered whether there was a legal basis, under the grounds of the 'legitimate interests' of the data controller or a third party under Section 2A(1)(d) of the Acts, for the bar to process the complainant's personal data by providing the CCTV footage to the employer organisation. This provision allows for the processing that is 'necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject'.

In its analysis of this case, the DPC had regard to the judgment of the CJEU in the Riga regional security police case in which the CJEU had considered the application of Article 7(f) of the Data Protection Directive (95/46/EC) on which Section 2A(1)(d) of the Acts is based, and identified three conditions that the processing must meet in order to justify the processing as follows:

a) There must be the existence of a legitimate interest justifying the processing;

b) The processing of the personal data must be necessary for the realisation of the legitimate interest; and

c) That interest must prevail over the rights and interests of the data subject.

The DPC established during its investigation that, arising from the incident in question, there was an allegation of a serious assault committed by the complainant against a colleague and the bar had provided a copy of the CCTV footage to the complainant's employer so that the employer could properly investigate that incident and the allegations made. The DPC took into account that as the incident had occurred during the employer organisation's workplace social event, the employer might have been liable for any injuries to any employee that could have

occurred during the incident. Accordingly, the CCTV was processed in furtherance of the employer organisation's obligation to protect the health and safety of its employees. As the CJEU has previously held that the protection of health is a legitimate interest, the DPC was satisfied that there was a legitimate interest justifying the processing. The DPC also considered that the disclosure of the CCTV in this instance was necessary for the legitimate interests pursued by the employer organisation so that it could investigate and validate allegations of wrongdoing against the complainant. The DPC considered, in line with the comments of Advocate General Bobek in the Riga regional security police case, that it was important that data protection is not utilised in an obstructive fashion where a limited amount of personal data is concerned. In these circumstances the DPC considered that it would have been unreasonable to expect the bar to refuse a request by the employer organisation to view and take a copy of the CCTV footage, against a backdrop of allegations of a serious assault on its premises, especially where the personal data had been limited to the incident in question and had not otherwise been disclosed. On the question of balancing the interest of the employer organisation against the complainant's rights and interests, the DPC had primary regard to the context of the processing, where the bar had received a request for the viewing and provision of a serious incident on its premises, which it had deemed grave enough to report to An Garda Síochána. A refusal of the request might have impeded the full investigation of an alleged serious assault, and the employer organisation's ability to protect the health and welfare of its employees. Accordingly the DPC considered that it was reasonable, justifiable and necessary for the bar to process the CCTV footage by providing it to the employer organisation, and that the legitimate interest of the employer organisation took precedence over the rights and freedoms of the complainant, particularly given that the processing did not involve sensitive personal data and there had not been excessive processing.

On the facts, the DPC was also satisfied that the bar currently had adequate signage alerting patrons to the use of CCTV for the purpose of protecting staff and customers and preventing crime, and that in the absence of any evidence to the contrary offered by the complainant, the complainant had been on notice of the use of CCTV at the time in question.

In many of the complaints that the DPC handles, data subjects hold the mistaken belief that because they have not consented to the processing of their personal data, it is de facto unlawful. However, there are a number of legal bases other than consent that justify processing depending on the particular circumstances. With regard to the legitimate interests justification, the DPC will rigorously interrogate whether the circumstances of the processing satisfy the elements that the CJEU has indicated must be present for controllers to rely on this legal basis. Equally, however, the DPC emphasises that where the circumstances genuinely meet the threshold required for this justification, as per the sentiment of Advocate General Bobek of the CJEU, protection of personal data should not disintegrate into obstruction of genuine legitimate interests by personal data.

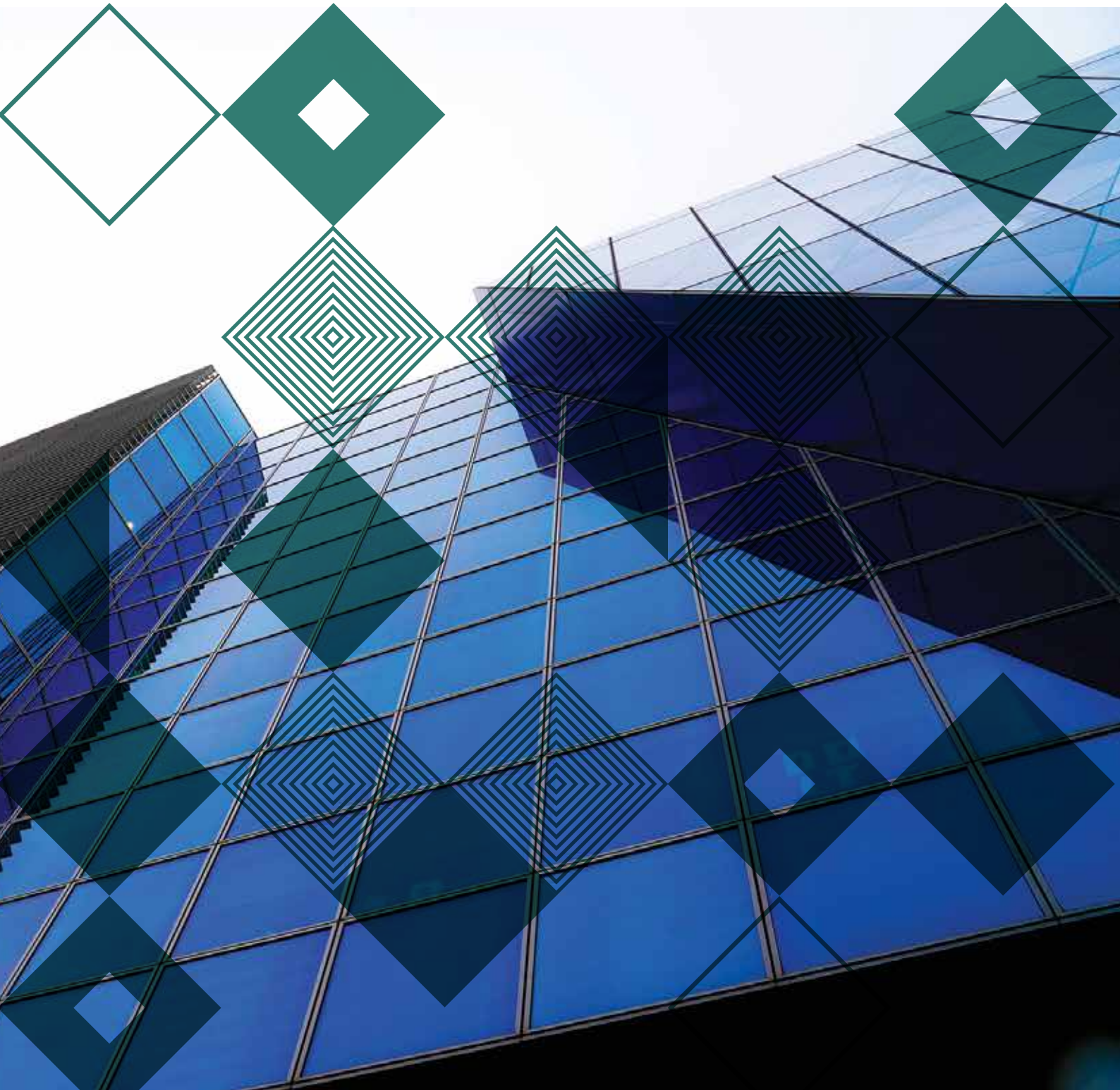
CASE STUDY 3
Ryanair web-chat transcript sent to another customer
(Applicable law — GDPR & Data Protection Act 2018)

We received a complaint from a data subject whose web-chat with a Ryanair employee was accidentally disclosed by Ryanair in an email to another individual who had also used the Ryanair web-chat service. The transcript of the web-chat contained details of the complainant's name and that of his partner, his email address, phone number and flight plans. The complainant told us that he had been alerted to the disclosure by the individual who had been erroneously sent the transcript of his web-chat.

In our examination of the complaint, we established that Ryanair's live web-chat service is provided by a third party, which is a data processor for Ryanair. We also established that the system that sends the web-chat transcripts by email has an auto-fill function that populates the recipient field with the email address of the last customer emailed. On the date in question, the data processor received requests from four Ryanair customers for transcripts of their web-chats, all of which were processed by the same agent. However, the agent did not correctly change the recipient email address when sending each transcript so that they were sent to the wrong recipients. Ryanair informed us that in order to prevent a recurrence of this issue the auto-fill function in the live web-chat system has

been disabled by the data processor and refresher GDPR training has been provided to staff.

Many of the complaints that the DPC receives relating to unauthorised disclosure of personal data in an electronic context — e.g. emails containing personal data sent to the wrong recipient — stem from use of the auto-fill functions in software. While data controllers may consider this a useful timesaver tool in a data-entry context, it has inherent risks when it is used to populate recipient details for the purposes of transmitting personal data. Auto-fill functions should therefore be used with caution, and where controllers decide to integrate such a function into their software for data-processing purposes, at a minimum other safeguards should be deployed, such as dummy addresses at the start of the address book, or on-screen prompts to double-check recipient details. The principle of safeguarding the security and confidentiality of personal data goes hand in hand with data protection by design and default so that when data controllers and processors are devising steps in a personal-data-processing programme or software, the highest standards of protection for the personal data are built in, particularly with regard to assuring the integrity, security and confidentiality of personal data.



Amicable Resolution

Under the Data Protection Act 2018 (the 2018 Act) the DPC may, where it considers there is a reasonable likelihood of the parties to a complaint reaching an amicable resolution within a reasonable timeframe, take steps to arrange or facilitate the amicable resolution of a complaint. In practice, the amicable resolution of a complaint may be facilitated at any stage of the complaint-handling process within the DPC where the parties are willing to have the complaint handled in this way.

Once the DPC identifies a complaint that can be amicably resolved, the possibility of a resolution is dependent on the willingness of the parties concerned to work through the substance of the complaint, such a process being facilitated by the DPC.

There are many ways in which a complaint might be amicably resolved. For example, in some cases, this could involve a gesture on the part of the data controller, or the issuing of an apology, but equally a complaint might also be resolved through the clarification of an issue to the satisfaction of both parties.

In the DPC's experience, a high proportion of complaints it handles are amenable to being amicably resolved in a timely fashion without the DPC's having to consider whether it should exercise its formal powers under the 2018 Act. However, even where a complaint has been resolved amicably — i.e. to the satisfaction of the complainant — the making of the complaint might have brought wider or systemic compliance issues within the data controller/processor organisation to the attention of the DPC. Where the DPC has been alerted to such issues, it has a range of other audit and investigatory powers at its disposal outside of the complaint-handling mechanisms under the 2018 Act (for example, it can open an inquiry of its own volition into the issues or conduct an audit) to further address the core issues identified.

Amicable Resolution Case Studies

Fundamental to the DPC's complaint-handing obligations is the vindication of the rights of data subjects. In the DPC's experience, the majority of individuals are satisfied when the behaviour of the data controller complained about is addressed. In handling complaints, wherever possible, by way of amicable resolution, the DPC can bring about optimum outputs for the maximum number of people who make complaints to the DPC by deploying its resources towards having the organisation complained about rectify the harm or the risk that has been posed to a data subject by the organisation's processing of the personal data.

CASE STUDY 4
Unlawful processing arising from billing error
(Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

In April 2018, we received a complaint from a data subject who had ceased to be a customer of the data controller. However, she had discovered that her data was still being processed as she continued to receive bills from the data controller. The complainant had received verbal and written assurances that she did not owe the amount being billed.

However, he complainant subsequently received a text message from a debt-collection company, asking that she contact them. When the complainant phoned the debt-collection company, it refused to provide her with any information regarding the alleged debt until she provided them with personal data verifying her identity, which she refused to do. Later the same day, the complainant received a letter from the debt-collection company confirming that it was seeking to recover monies owed by her to the data controller.

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

Company A confirmed with the DPC that an error had caused the complainant's account balance to appear outstanding but that when the error was identified by the data controller, the outstanding balance was removed from the account. The data controller also confirmed that it had instructed the debt-collection company to cease any collection activities, and also to delete any data associated with the complainant.

While the complainant was satisfied with the ultimate outcome, the DPC emphasised to the data controller that the complainant had previously been informed on at least two occasions that the matter had been resolved. Despite this, her data had been unfairly processed by being passed to a debt-collection company without there being any justification for such disclosure.

In recognition of its failings, the data controller apologised to the complainant, provided certain assurances to her that the matter would have no effect on her credit rating, and made donations to charities of her choice.

For a controller to lawfully engage a processor to process personal data, there must be a justification for the processing of the personal data in the first place. In this case, the controller had disregarded previous concerns raised by the complainant that bills were being issued to her despite her no longer receiving services from the controller and had failed to look into the continued use of her personal data for billing purposes in circumstances where she was no longer a customer. The DPC encourages individuals to raise data protection concerns directly with the controller in the first instance so that they can address them. However, data controllers frequently ignore or disregard direct attempts made by a data sub-

ject to raise complaints until the DPC becomes involved. This is unacceptable and, as part of each organisation's accountability obligations, it should have meaningful and efficient measures in place to deal with and address data protection complaints when raised directly by a data subject, without the need for the data subject to resort to DPC intervention.

CASE STUDY 5
Late response to an access request
(Applicable law — GDPR & Data Protection Act 2018)

The GDPR places timelines on data controllers to respond to requests from data subjects when they are exercising their rights. In the case of one data subject who requested a recording of a telephone call conducted between the data subject and the customer-service operator line of a multinational technology company in order to progress a customer-service complaint, a complaint was made to the DPC that the access request submitted pursuant to Article 15 of the GDPR had not been processed within the timeframe set out by the GDPR.

Upon receipt of the complaint, the DPC contacted the company concerned to make it aware of the complaint and to enquire as to whether there was any action it would like to take on this matter. The company responded to the data subject with a copy of the requested telephone call and, accordingly, the data subject was satisfied for the complaint to be amicably resolved. Based on the circumstances of this individual case, the DPC deemed no further regulatory action necessary.

CASE STUDY 6
Access request to golf club for CCTV
(Applicable law — GDPR & Data Protection Act 2018)

In November 2018, we received a complaint from a data subject in relation to an access request for his personal data comprising CCTV footage for a particular time and date, made to a golf club, the data controller.

The data subject provided us with initial correspondence from the golf club asking him why he required the footage and subsequent correspondence informing him that it had discovered a problem with the CCTV system software and was unable to provide him with the requested footage.

This complaint was deemed potentially capable of being amicably resolved under Section 109 of the Data Protection Act 2018.

As part of the amicable resolution process, we sought an explanation from the golf club as to why the requested CCTV could not be provided to the complainant.

The golf club informed us that its CCTV system was not operational on the date for which the data subject had requested footage, and that this had only been discovered when it sought to comply with the access request. The DPC was not satisfied with the generality of this explanation and required a more detailed written explanation on the issues affecting the CCTV, which could also be shared with the complainant. In response to this request, we were supplied with a letter from the golf club's security

company that outlined the issues with the CCTV system, including the fact that the hard drive on the CCTV system had failed and that the system had not been in use for some time. The DPC was satisfied with the technical explanation provided and golf club agreed that this letter could be shared with the complainant. The complainant was satisfied with the explanation, leading to an amicable resolution.

This case illustrates that even when working towards the facilitation or arrangement of an amicable resolution of a complaint, the DPC still expects accountability on the part of the controller or processor, and will scrutinise explanations and reasons given as to non-compliance with its obligations in order to ensure that the position put forward is verifiable and demonstrable.

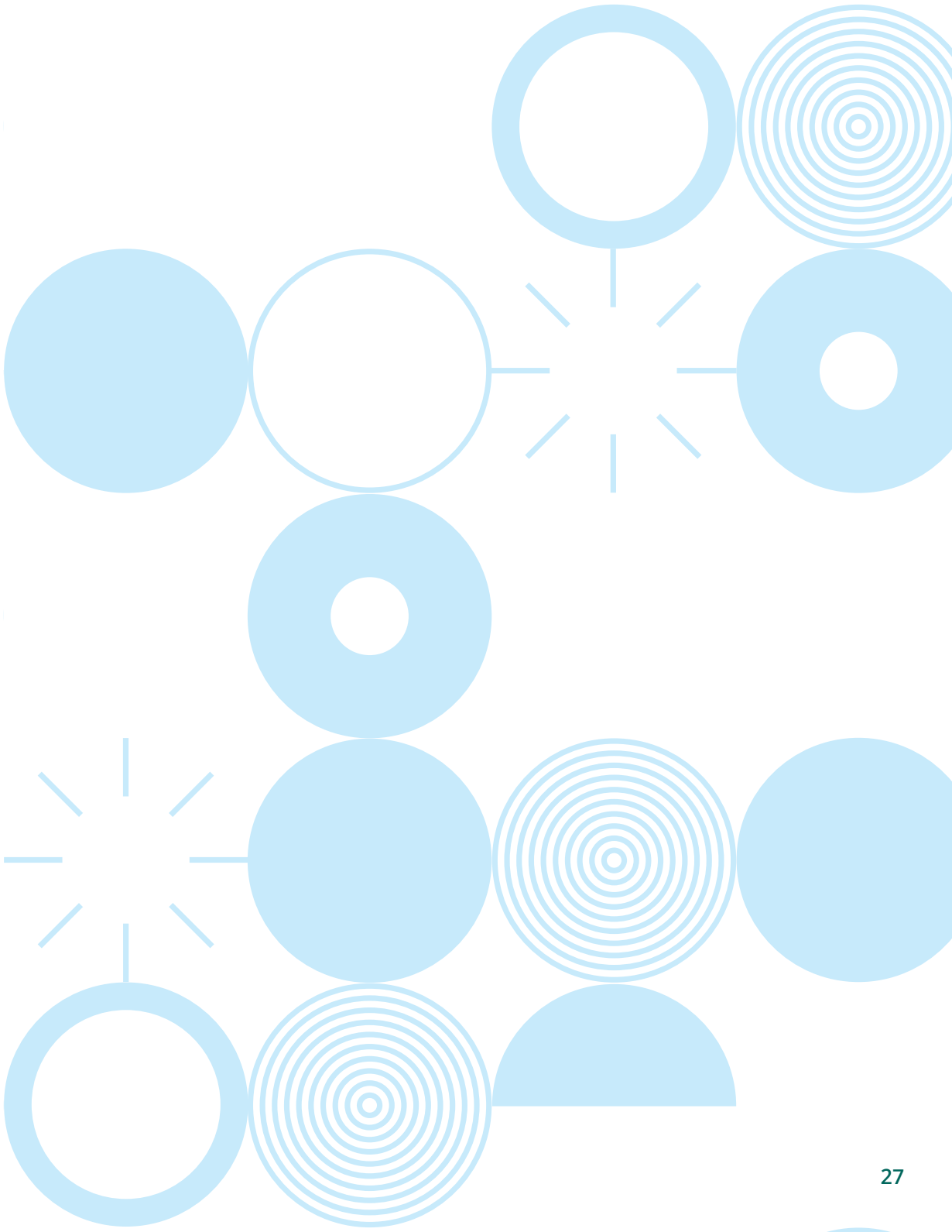
CASE STUDY 7
Financial information erroneously cc'd to a restaurant
(Applicable law — Data Protection Acts 1988 and 2003 (the Acts))

We received a complaint concerning the alleged disclosure by a motor dealership of the complainants' personal data to a third party. The complainants had provided the dealership with copies of their driver's licences and bank details, including bank statements and full account details, in order to purchase a car through a Personal Contract Plan. They were subsequently copied in on an email from the dealership to a third-party email address, believed to be an address associated with a bank, which contained the complainants' driver's licences and bank details. The complainants were concerned that the third-party address was that of a restaurant and contacted the dealership about this, but were assured that the email address in question pertained to a bank and was secure.

The complainants remained concerned over the ownership of the email address, conducted online research into the matter, and were confident the email address was that of a restaurant. In order to confirm their suspicions, a friend of the complainants sent an email to the address in question and the response received confirmed it was that of a restaurant.

In the course of our examination, the dealership accepted that the email had been sent in error to the wrong address. Notwithstanding this acknowledgment, it was clear that no attempt had been subsequently made to contact the restaurant in order to request that the information erroneously sent be deleted by the unintended recipient. Upon instruction from this office, we received confirmation that the dealership had contacted the restaurant and requested that the email, including the documents, be deleted. The dealership put forward a proposal for amicable resolution that was accepted by the complainants.

This case demonstrates that it is vital for data controllers (and their employees) to implement and ensure a practice of precautionary measures when electronically transmitting personal data, particularly financial information. A large proportion of the data-breach notifications that the DPC receives are of the unauthorised-disclosure variety, with a common cause being emails sent in error to the wrong address. Where a data controller identifies that such an incident occurs, it is not enough to acknowledge it, whether to the data subject or to the DPC. Instead, it is incumbent on the data controller to take all reasonable steps to remedy such a breach. This includes recalling the email from the sender, asking the unintended recipient to confirm they have deleted the email, and thereafter putting in place measures to prevent a recurrence. Human error by staff presents a high risk of data breaches on an ongoing basis and it is critically important that efforts are made to mitigate those risks by driving data protection awareness throughout the organisation, particularly in regard to new staff.



Statutory Inquiries by the DPC

As mentioned above, under the Data Protection Act 2018 (the 2018 Act), 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. These are a complaint-based inquiry or 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 in the inquiry;
- 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[1].

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 materials[2]. 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.

1 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.

2 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.

General description of the phases of a statutory inquiry

Set out below in high level terms is a description of each phase of a statutory inquiry by the DPC where the DPC is acting as lead supervisory authority in relation to a cross-border processing issue, and a complaint has been lodged with the DPC directly, or the DPC has commenced an inquiry of its own volition.

This description is not binding on the DPC but is for general illustrative purposes only, showing the provisional sequencing of phases in an inquiry. It is not determinative of the precise steps which will be followed in each inquiry, which will depend on the nature, circumstances, scope and subject matter of the inquiry. The first wave of DPC inquiries under the GDPR and 2018 Act are currently ongoing but will be completed during 2019. As such, the provisional sequencing set out below, may be subject to changes arising from the crystallisation of the inquiry process, at both national and EU level, in those cases.

In part, this description is intended to demonstrate that it is not possible for the DPC to summarily apply fines or any other corrective powers. The conduct of an inquiry by the DPC must be in accordance with due process and fair procedures.

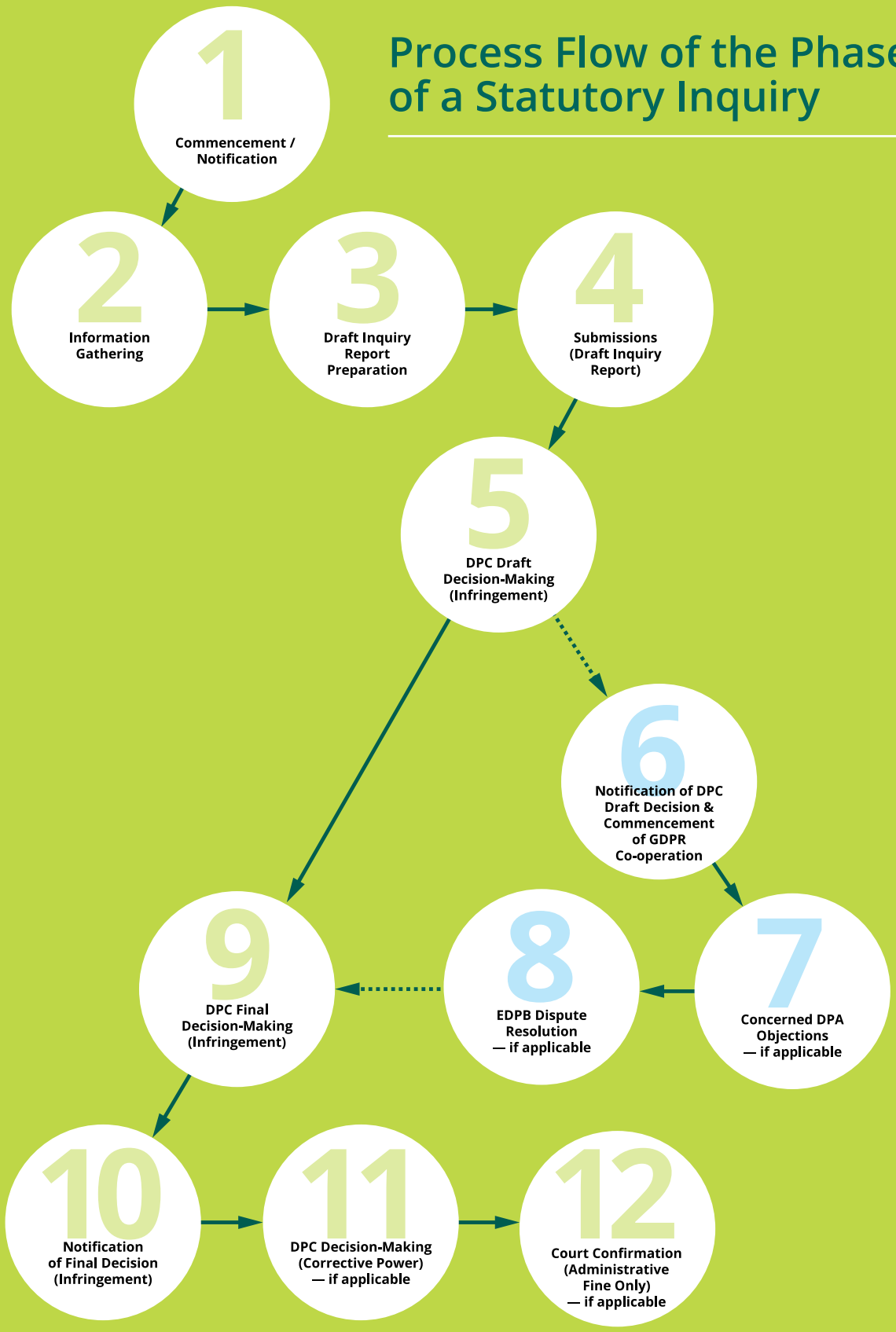
Inquiry phases for illustration purposes:

1. Commencement/ notification phase
    - Scope determination
    - Notification to controller/processor of inquiry commencement
    - Issuing of preliminary questions
2. Information gathering phase
    - DPC investigator gathers all relevant information/ documents/ materials from the parties — may be iterative.
3. Draft inquiry report preparation phase
    - DPC investigator completes consideration of information/ documents/ materials and factual and legal analysis and drafts inquiry report
    - Draft inquiry report sets out (a) findings of fact (b) application of the law under the GDPR and/or the 2018 Act to the findings of fact, and (c) draft findings, giving reasons for them, as to whether or not there has been one or more infringements of the law by the controller/ processor. The draft inquiry report will not comment on the application of corrective powers.

4. Submissions phase (draft inquiry report)
    - DPC investigator issues draft inquiry report to the parties
    - Parties make submissions on draft inquiry report
    - Investigator considers submissions and prepares finalised inquiry report for DPC decision-maker
5. DPC draft decision-making phase (infringement)
    - DPC decision-maker considers inquiry report
    - If deficiencies in investigation procedure or outstanding issues identified, DPC decision-maker remedies these
    - DPC decision-maker makes a "draft decision" (the DPC draft decision) in relation to whether there has been one or more infringements of the GDPR and/or 2018 Act.
6. Notification of DPC draft decision & commencement of GDPR co-operation phase
    - DPC decision-maker notifies DPC draft decision to other concerned EU data protection authorities (DPAs) via the IMI platform
7. Concerned DPA objections phase — if applicable
    - DPAs may raise any "relevant and reasoned objection" to the DPC draft decision
    - DPC decision-maker considers any such objections and may revise the DPC draft decision
8. EDPB Dispute Resolution phase — if applicable
    - EDPB dispute resolution triggered if DPC decision-maker considers it cannot implement a concerned DPA objection
    - EDPB votes by majority on subject matter of any "relevant and reasoned objection"
    - EDPB decision adopted by DPC decision-maker and DPC Draft Decision is revised, as required, under phase 9 below
9. DPC final decision making (infringement) phase
    - DPC decision is finalised
10. Notification of final decision (infringement) phase
    - Final DPC decision notified to parties, including any decision of the EDPB dispute resolution phase
    - Right of appeal by either party against the final decision
11. Decision-making phase (corrective power) — if applicable[3]
    - DPC decision-maker decides what corrective powers including administrative fines apply
    - May invite, if relevant, submissions of parties
    - Decision on corrective power notified to the parties
    - Right of appeal by controller/ processor against decision on corrective power
12. Court confirmation phase — if applicable (administrative fine only)
    - If administrative fine not appealed by controller/ processor within 28 days, DPC applies to the Irish Court to confirm fine

3. Phase 10 and 11 may occur as one combined phase.

Process Flow of the Phases of a Statutory Inquiry



Note: Solid line indicates sequence of national level steps and dotted line indicates pathway to and from EU/EDPB level, where applicable.

Complaint-handling Mechanisms under the New Legal Framework

One of the biggest changes brought about by the Data Protection Act 2018 (the 2018 Act), which gives further effect in Ireland to the provisions of the GDPR and the Law Enforcement Directive, is that now, where a complaint is not amicably resolved, the DPC is no longer legally obliged to make a formal, statutory decision on the complaint. Instead, there are a range of tools at the DPC's disposal for dealing with the complaint, such as providing advice to the complainant, or issuing one of a number of different types of enforcement notices against the data controller or processor — for example, directing them to comply with a request made by the complainant, such as a request for access to, or erasure of, personal data. Occasionally, where the DPC considers that there is justification for doing so, depending on the nature, gravity, duration or other factors or circumstances of the complaint, the DPC may open a statutory inquiry into the complaint and use its range of formal investigatory powers to examine the issues in the complaint further. As mentioned above, it is also possible for a second type of statutory inquiry to be opened (an inquiry of the DPC's own volition), which is not based on the specific complaint but that may examine thematic or systemic issues raised by the complaint relating to how, or to what extent, an organisation complies with data protection law. Where the DPC opens a statutory inquiry in relation to a specific complaint, that inquiry will generally result in a statutory decision of the DPC.

Irrespective of the complaint-handling or other tools that the DPC uses under the 2018 Act to deal with a complaint, the DPC will always issue a final communication to the complainant, informing them as to how their complaint has been handled and concluded.

Of the 1,928 GDPR-related complaints received during the period in question, and as of 31 December 2018, 510 complaints proceeded to complaint-handling; 550 complaints were open and being actively assessed by the DPC's Information and Assessment Unit; and 868 were concluded at the assessment stage, either as a result of the individual being able to resolve the matter directly with the data controller following receipt of the DPC's guidance, or as a result of the matter being withdrawn. Other reasons included the following: the matters complained of were outside the remit of the DPC because they did not relate to the processing of personal data; and the individuals did not pursue their concerns further with the DPC. A further 612 complaints were concluded by the DPC between 25 May and 31 December 2018 under the Data Protection Acts 1988 & 2003.

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 or carry out their activities in more than one EU member state deal with data protection authorities (called 'supervisory authorities' under the GDPR). The OSS principle requires that organisations with multiple establishments across different member states of the EU are subject to regulatory oversight by just one DPA, where they have a 'main establishment' in the EU and are engaged in 'cross-border processing', rather than being subject to regulation by the data protection authorities of each member state in which they have establishments. The main establishment of an organisation will generally be its place of central administration (e.g. its headquarters). However, in the case of a data controller, if decisions are taken on the processing of personal data somewhere else in the EU, then that other place in the EU will be its main establishment. In the case of a data processor, if it has no place of central administration, then its main establishment will be where its main processing activities in the EU take place.

Under the GDPR, cross-border processing involves one of two scenarios. The first is where a data controller or processor is established in more than one member state and processing takes place in the context of the activities of more than one such establishment. The second scenario captures a situation where the data controller or processor is established in just one member state but the processing substantially affects, or is likely to substantially affect, data subjects in more than one member state. In either of those scenarios, the concept of the 'lead supervisory authority' under the GDPR will apply to determine the DPA that has primary responsibility for dealing with a complaint or an issue that has arisen in relation to cross-border processing. Under the rules of the GDPR, the DPA in the member state where the multinational organisation has its 'main establishment' (as discussed above) will act as the lead supervisory authority, making that multinational subject to only one set of regulatory actions rather than multiple actions by different data protection authorities of different member states in the event that the multinational infringes one or more provisions of the GDPR.

The role of the lead supervisory authority 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 a concerned supervisory authority where: a cross-border processing complaint has originally been lodged with the DPC but another DPA is the lead supervisory authority; or where the processing in question substantially affects, or is likely to substantially affect, data subjects in Ireland; or where the controller/processor is established in Ireland.) This means that the lead supervisory authority must not only take 'utmost account' of the views of the DPA which received the complaint when preparing a draft decision, but also then 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 EDPB making a majority decision on the disputed issues in the draft decision.

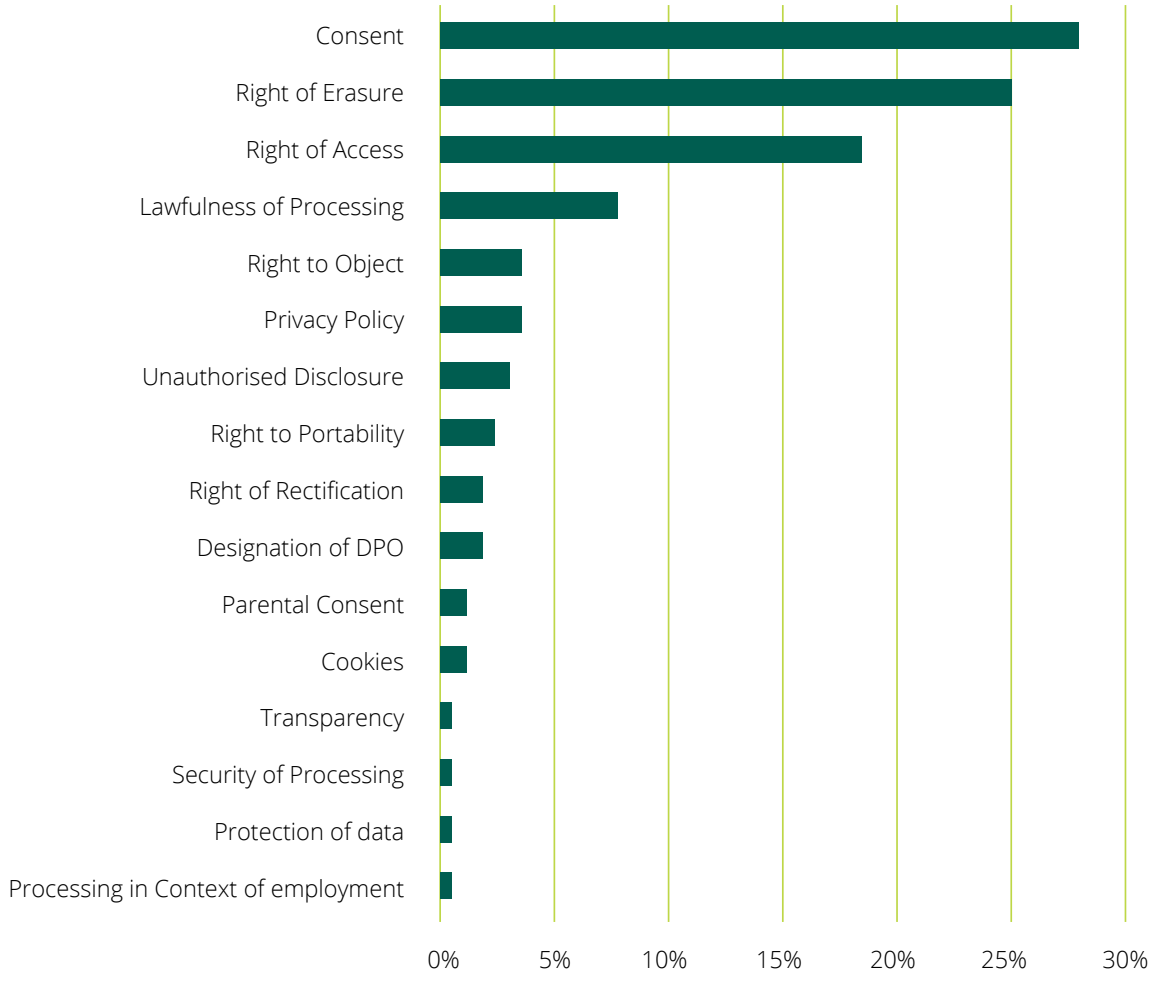
Under the OSS mechanism, the DPC is the lead supervisory authority for a broad range of multinationals, including many large technology and social media companies, whose main establishment is located in Ireland. As a lead supervisory authority, the DPC now handles complaints originally lodged with other EU data protection authorities, in addition to handling complaints lodged by individuals directly with the DPC. Between 25 May and 31 December 2018, the DPC received 136 cross-border processing complaints through the OSS mechanism that were lodged by individuals with other EU data protection authorities. This new channel for receiving complaints requires close cooperation and information exchange between the DPC and the EU DPA with which the complaint is lodged because the complainant communicates directly with the DPA where the complaint was lodged. In practice, this means that all updates on the progress of a cross-border processing complaint must be transmitted by the DPC to the receiving DPA, who will then translate the update into the relevant national language, where required, and issue it to the complainant.

Breakdown of cross-border complaint types received by the DPC through the OSS mechanism

Law Enforcement Directive (LED) Complaints

The GDPR does not apply to any processing of personal data that is carried out for law-enforcement purposes by authorities with law-enforcement powers. Instead, an EU directive known as the Law Enforcement Directive (Directive (EU) 2016/680) (the LED) was implemented at EU level to sit alongside the GDPR and operate in parallel with it. The LED was transposed into Irish law by way of certain parts of the Data Protection Act 2018 (the 2018 Act). Processing of personal data for law-enforcement purposes is broadly covered in Part 5 (Sections 69 to 104) while Chapter 3 of Part 6 (Sections 118 to 128) of the 2018 Act deals with enforcement of the LED. In addition, other parts of the 2018 Act simultaneously apply to the GDPR and the LED.

In broad terms, the LED applies where a data controller is a 'competent authority' within the meaning of the 2018 Act 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. In Ireland, many public authorities and bodies have law-enforcement functions and processing by them for the purposes of PIDP of criminal offences or the execution of criminal penalties will be captured by the LED as transposed under the 2018 Act.



However, it is important to note that where a competent authority processes personal data other than for these purposes, the GDPR (and the relevant provisions of the 2018 Act that give further effect to the GDPR), not the LED, will apply.

The enactment of the 2018 Act saw the establishment of a new LED Complaints Unit and the development of a two-step test to assist the LED Complaints Unit in determining whether the processing in question is within the scope of the LED and Part 5 of the 2018 Act. The two-step test requires the following criteria to be met:

- The data controller responsible for the processing in question must be a 'competent authority' as defined by Section 69 of the Act.
- The processing in question must be for 'law enforcement purposes' as defined in Section 70 of the Act.

If the first step of this test is met, but not the second, then — although the controller may ordinarily be a competent authority for the LED and Part 5 of the Act (such as An Garda Síochána) — the processing in question is deemed not to fall under the scope of the LED. In such a case, the non-law-enforcement processing being carried out by the competent authority will likely fall within the scope of the GDPR legislative regime (for example, processing for Garda HR matters).

Between 25 May and 31 December 2018, the DPC handled seven LED complaints, six of which entailed An Garda Síochána as the data controller. In one complaint, disclosure of an individual's data by a local authority occurred in error, with the disclosure relating to the investigation of an offence prosecutable by the local authority, thereby falling under the LED.

Data-Breach Complaints

One type of complaint received by the DPC is that of data breaches. These can materialise from circumstances where a data subject has become independently aware of a data breach, e.g. through media coverage of a data breach affecting an organisation that is processing their personal data, or through adverse impacts upon them directly as a result of a data breach (e.g. unauthorised access to email accounts, customer or bank accounts, etc.), or by way of a notification to them from the data controller that there has been a breach in relation to their own personal data.

Where a breach has been notified to the data subject by the data controller but not to the DPC, the Breach Complaints Unit will ensure the breach is retrospectively reported to the Breach Notifications Unit, accompanied by a clarification from the data controller/processor as to why the DPC was not notified in the first instance. In certain cases where the issue of non-reporting is queried by the DPC, some data controllers indicate the assignment of 'minimal risk' to the data breach once it has been detected, and indicate that the data has been secured and the data subject informed if deemed necessary. When assessing the necessity of notifying breaches, the DPC advises data controllers that cognisance is given to the impact of a data breach on the rights and freedoms of a data subject.

Between 25 May and 31 December 2018, the DPC handled 48 data-breach complaints from affected data subjects. In most cases, the data breach concerned the personal data of an individual being issued to another third party in error. Unfortunately, in some of these cases the third party was an ex-partner or a relative of the affected individual. Several breach complaints concerned more systemic breaches where a high number of individuals were affected. In all cases, the DPC requires the controller to provide it with a fulsome explanation as to how the breach occurred and to convey the explanation to the data subject. The DPC also requires the data controller to outline all steps taken to mitigate future recurrence. The taking of such steps may lead to the amicable resolution of the matter and may preclude the need for the DPC to exercise its formal statutory powers. However, in cases of high impact or severe gravity from a systemic perspective, a statutory inquiry may be commenced, whether of the DPC's own volition (this will be so in the majority of cases) or in relation to the particular circumstances of an individual complaint.

Data-Breach Complaints Case Study

CASE STUDY 8
CSO data breach — Disclosure of P45 data
(Applicable law — Data Protection Acts 1988 and 2003)

We received several complaints in late 2017 against the Central Statistics Office (the CSO), each alleging that the CSO had disclosed the respective complainants' personal data without their consent or knowledge. The complaints related to a data breach that the CSO had previously reported to us (under the voluntary Personal Data Breach Code of Practice) and to the affected individuals.

The data breach originated from actions taken by the CSO in response to three requests over a five-day period from separate former census enumerators seeking their P45 information. Emails with PDF attachments containing their own P45 and P45s of thousands of third parties were sent to the requesting enumerators. The CSO informed us that the data breach had been identified when a member of CSO staff had reviewed the relevant CSO sent-items mailbox, as part of the CSO's standard due-diligence practices. The CSO confirmed that the disclosed third-party P45 information contained personal data including PPSNs, dates of birth, addresses and details of earnings from employment as census enumerators.

During our investigation, the CSO informed us that upon discovering the breach it had notified the recipients of the error, who had subsequently confirmed in writing that they had deleted the files. The CSO told us that it had also notified the affected individuals of the facts of the breach as they pertained to each individual. The CSO also informed us that following the data breach it had implemented a range of new procedures for handling P45 requests, including a rule that P45 requests were to be answered only by post going forward.

This data breach had impacted on the thousands of individuals whose personal data was contained in the files that were unlawfully disclosed to the three former enumerators. The incident essentially occurred in triplicate because the erroneously disclosed files had been attached to three separate outgoing communications. This incident would have been preventable had the CSO had the appropriate processes in place for the oversight of releasing tax-related personal data.

The DPC issued a number of individual decisions in respect of complaints in relation to this breach, finding in each case that a contravention of Section 2A(1) of the Data Protection Acts 1988 and 2003 had occurred, in that personal data had been processed without a legal basis, as was clear from the breach report submitted to the DPC from the CSO. Having examined the new measures implemented by the CSO to guard against a recurrence, the DPC was satisfied that they comprehensively addressed the failings that had brought about this incident. However, from the perspective of ensuring the lawfulness of the processing and the security and confidentiality of personal data held by the CSO, those new organisational procedures only served to underline the inadequacy of the previous measures for responding to requests for tax-related information.

4 Data-Breach Notifications

Since 25 May 2018, a new mandatory data-breach notification obligation has applied to all organisations that are data controllers. This legal requirement accounts for most breach notifications received by the DPC.

Separately, a mandatory 24-hour breach notification obligation applied, and continues to apply, to telecommunications and internet service providers under the e-Privacy Regulations (S.I. No. 336 of 2011) and Commission Regulation (EU) No. 611/2013. Prior to 25 May 2018, most reported personal-data security breaches were submitted to the DPC under a voluntary — i.e. not legally binding — Personal Data Security Breach Code of Practice, which was introduced in July 2011 and that ceased to apply from 25 May 2018. However, the DPC has continued to receive breach notifications in accordance with the Personal Data Security Breach Code of Practice that occurred prior to that date but that were reported to the DPC on or after 25 May 2018. Finally, the DPC also receives breach notifications in relation to the mandatory notification requirement under the LED transposed by way of certain parts of the Data Protection Act 2018 (see the section on the Law Enforcement Directive for further details).

Between 25 May and 31 December 2018, the DPC received 3,687 data-breach notifications under Article 33 of the GDPR, of which 145 cases (4%) were classified as non-breaches as they did not meet the definition of a personal-data breach as set out in Article 4.12 of the GDPR. A total of 3,542 valid data protection breaches, across all four legal frameworks, were recorded by the office between 25 May and 31 December 2018, representing an increase of 27% (747) on the numbers reported in 2017.

As in other years, the highest category of data breaches notified under the GDPR were classified as Unauthorised Disclosures and accounted for just under 85% of the total data-breach notifications received between 25 May and 31 December 2018. The majority occurred in the private sector (2,070).

The DPC received a total of 92 valid data-breach notifications under the e-Privacy Regulations (S.I. No. 336 of 2011 — see details above), which accounted for just over 2% of total valid cases notified for the year.

Breaches Involving Multinational Technology Companies

In the period between 25 May and 31 December 2018, the DPC was notified of 38 personal-data breaches involving 11 multinational technology companies. (It should be noted that data-breach notifications involving companies in the multinational technology sector are examined and handled by the Technology & Multinationals Unit rather than by the Data Breach Unit.) A substantial number of these notifications involved the unauthorised disclosure of, and unauthorised access to, personal data as a result of bugs in software supplied by data processors engaged by the organisations. The DPC commenced several formal statutory inquiries on receipt of these notifications (for example, the Facebook Token breach in September 2018), some of which were the subject of much media coverage and public comment (see the Technology Multinationals Supervision section of this report). In general terms, these inquiries examine whether the relevant organisation discharged their GDPR obligations, including the obligation to implement technical and organisational measures to secure and safeguard the personal data they process.

By way of general comment, the GDPR emphasises the need to implement protective measures (both technical and organisational) that correspond to the level of risk of the processing that an organisation may undertake. Organisations should continuously evaluate their technical and organisational security position and should refine their technical and organisational measures in accordance with the risk. In this context, the DPC recommends that organisations ensure that they:

- are not overly reliant on data processors to implement appropriate security measures relating to personal-data processing and satisfy themselves that the security measures in place with their data processors are appropriate to the risk posed by the relevant data-processing activities. An organisation should also be able to demonstrate to the DPC that it is satisfied with the technical and organisational measures implemented by any data processor it engages;
- have appropriate data-processing agreements in place that assure good governance and controls regarding data processors, and that data processors have complied with their obligations to securely process personal data on the instruction of the data controller; and
- are not over reliant on data processors regarding the determination and implementation of appropriate security measures to protect an organisation's personal-data processing. Active and ongoing engagement with data processors to ensure that its technical and organisational measures are appropriate to the risk and meet the organisation's specific security requirements to protect the processing of personal data is critical.

LED breach notifications

The DPC also received 12 breach notifications in relation to the LED, (Directive (EU) 2016/680), which has been transposed into Irish law, by certain parts of the Data Protection Act 2018.

Typical examples of data breaches notified between 25 May and 31 December 2018 to the DPC included:

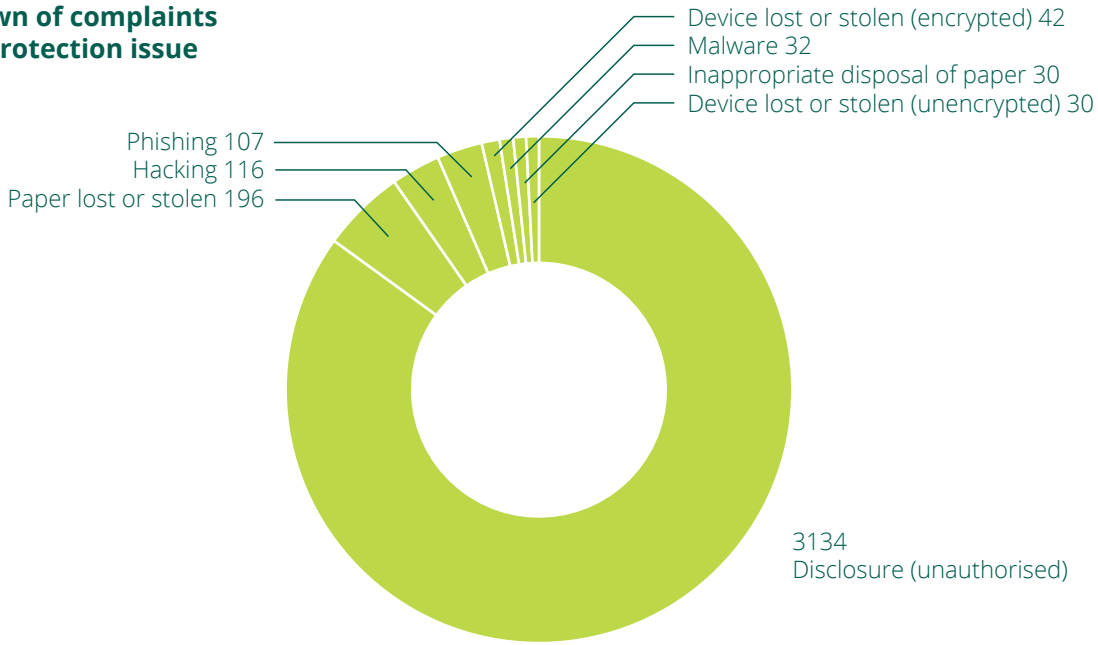
- inappropriate handling or disclosure of personal data, e.g. improper disposal, third-party access to personal data - either manually or online, unauthorised access by an employee;
- loss of personal data held on smart devices, laptops, computers, USB keys and paper files; and
- malicious or criminal cyber incidents such as brute-force attacks, hacking, malware, phishing and ransomware.

As was the case in 2017, there was a rise in the number of cyber security compromises notified with the number of notifications increasing sharply from 49 cases in 2017 to 225 in 2018. Cases such as these include phishing, malware and ransomware attacks.

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

Data-breach notifications by category (2018)	Private	Public	Grand Total
Device lost or stolen (encrypted)	21	21	42
Device lost or stolen (unencrypted)	17	13	30
Disclosure (unauthorised)	2070	1064	3134
Hacking	102	14	116
Inappropriate disposal of paper	15	15	30
Malware	27	5	32
Paper lost or stolen	86	110	196
Phishing	91	16	107
Grand Total	**2429**	**1258**	**3687**

Breakdown of complaints by data protection issue



The following case studies represent a sample of the different types of data breaches notified to the DPC between 25 May and 31 December 2018. Each one could have been prevented had the organisation implemented appropriate technical and organisational measures as per Article 32 of the GDPR.

Data Breach Case Studies

CASE STUDY 9
Failure to implement the data protection policies in place

An employee of the data controller, a public-sector body, lost an unencrypted USB device containing personal information belonging to a number of colleagues and service users.

The public controller had the appropriate policy and procedures in place prohibiting the removal and storage of personal data from its central IT system by way of unencrypted devices. However, it lacked the appropriate oversight and supervision necessary to ensure that its rules were complied with, and the employee appeared not to have been aware of the policy regarding the use of unencrypted devices. The breach could have been prevented had the organisation fully implemented the policy and made staff aware of it.

CASE STUDY 10
Unencrypted USB device lost in the post

A private-sector data controller notified the DPC that a package containing consent forms and an unencrypted USB device had been sent using standard postal services.

However, the package was damaged in transit, causing the USB device to fall out and become lost. The USB device contained pictures of minors participating in an organised educational event. The potential loss/disclosure of the personal data contained on the USB device could have been prevented/mitigated had the data controller had in place and implemented an encryption policy surrounding the used of portable memory devices and an adequate policy concerning sending sensitive material through the post, e.g. registered post/courier service.

CASE STUDY 11
Website phishing

A private sector (educational) data controller reported an incident of phishing, where a staff member had clicked on a suspicious website link and entered their credentials resulting in their email account becoming compromised.

The data controller had not enabled multi factor authentication on its email accounts. Had this technical measure and appropriate cyber security training been in place from the outset this data breach may have been preventable.

CASE STUDY 12
Loss of paper files in transit

The data controller, a public body, notified the DPC about an incident involving the transportation of hard-copy legal files containing special-category personal data.

The controller had contracted a courier company to transport the files to another department but the files went missing in transit. It transpired that the controller did not retain a backup of the original files, resulting in a loss of personal data. The controller did not have sufficient procedures in place for the secure removal and storage of hard-copy files that contained special-category personal data. The breach could have been prevented had the organisation properly considered its requirements when transporting such materials to another location and the inherent risks involved in such activities, and implemented more secure measures to ensure the protection of personal data.

CASE STUDY 13
SIM swap attack

A data subject notified the data controller (a mobile-phone network operator) that a SIM card swap was requested and authorised on her mobile-phone account by an unauthorised third party.

The data subject was concerned because her mobile-phone number had been used to receive text messages for two-factor authentication from her bank in relation to her banking service. Further investigation undertaken by the data controller indicated that an unknown third party had obtained limited personal data belonging to the data subject by some external means and had managed to pass the controller's identity-validation processes. The customer-service agent for the data controller did not follow the validation process fully, and facilitated a SIM card swap on the customer's account contrary to the controller's policy. The breach would not have occurred had the controller had more robust processes preventing access to key account information and the customer-service agent had received sufficient data protection training, including on the risks posed to customer personal data by deviating from the company's validation policy.

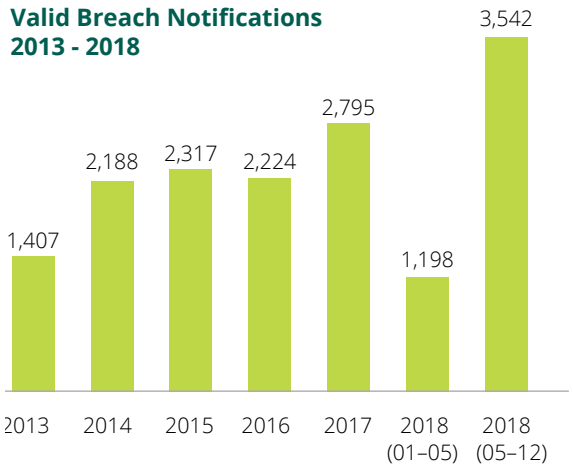
Comment on Prevalent Data Breaches

It is notable that many of the data breaches notified to the DPC involving a risk to financial data resulted from compromised or stolen credentials. In relation to the public-sector breaches notified to the DPC, it is of particular concern that a large number involved special categories of personal data or data relating to criminal convictions or offences.

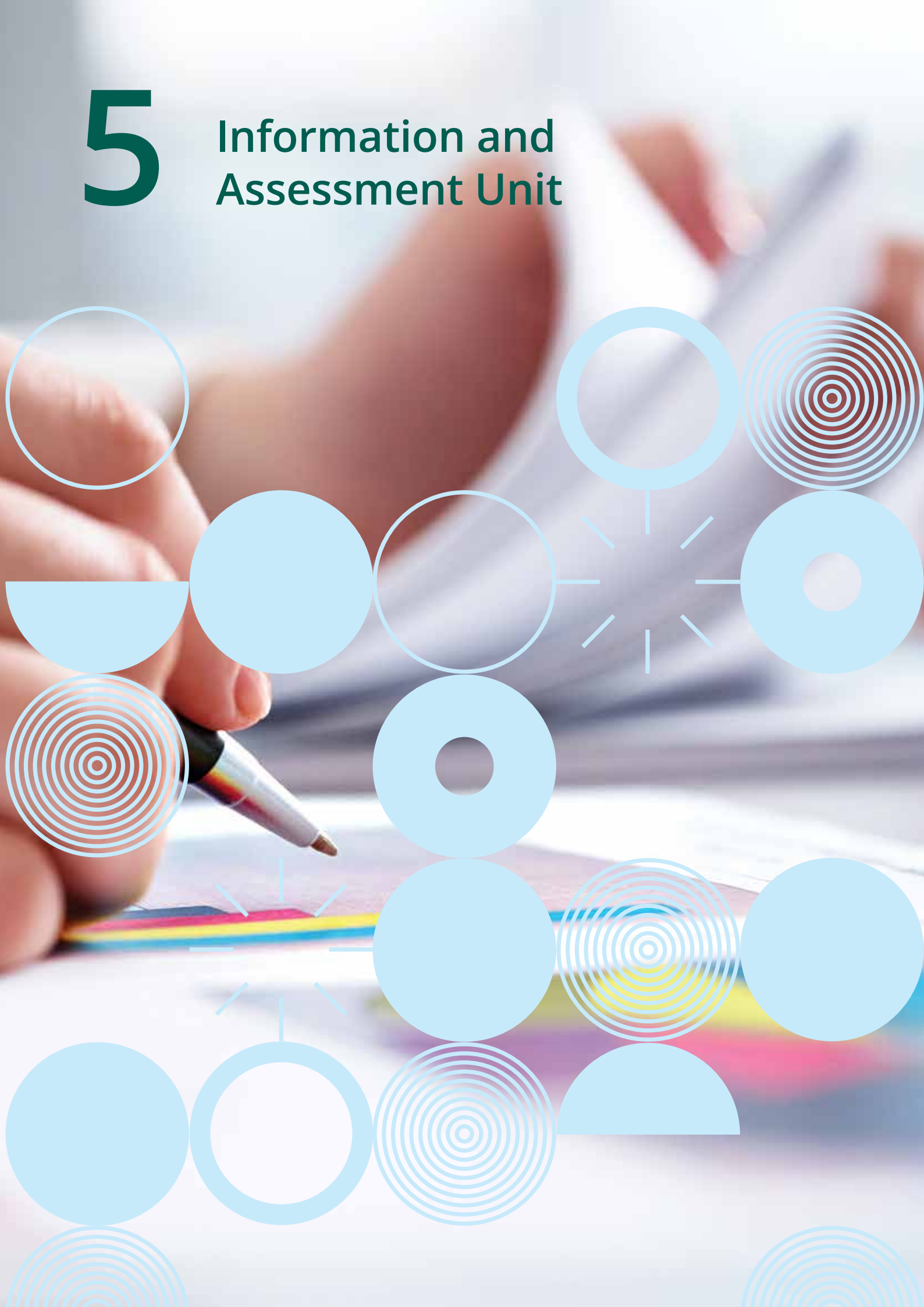
Controllers' and processors' security obligations mean they must take into account the nature, scope, context and purposes of processing as well as the different types of risks that might present during the processing of such data, and the likelihood and severity of those risks for the individuals whose personal data is being processed. The elevated nature of the inherent risks in processing special categories of personal data, data relating to criminal offences and convictions, and financial data means that controllers must implement higher-level technical and organisational measures to secure and safeguard such personal data. Those measures must be commensurate with the specific risks posed by the particular processing operations.

Arising out of certain patterns identified in data breaches notified to the DPC by particular controllers, the DPC has commenced seven own-volition inquiries under Section 110 of the Data Protection Act 2018 to date. In addition, the DPC is examining the specific circumstances of other breach notifications with a view to commencing statutory inquiries or prosecutions under the e-Privacy Regulations (S.I. No. 336 of 2011).

Valid Breach Notifications 2013 - 2018



5 Information and Assessment Unit



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.

The DPC's Information and Assessment Unit (IAU) 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, the unit also engages with individuals and assesses concerns and complaints received in relation to potential infringements of their data protection rights.

Responding to Queries

The introduction of the GDPR on 25 May 2018, and the corresponding increase in awareness of data protection issues among organisations and the general public, has resulted in a significant increase in the workload of the IAU. The IAU received almost 31,000 contacts comprising approximately 15,000 emails, 13,000 telephone calls and 3,000 items of correspondence via post between 25 May 2018 and 31 December 2018.

At the DPC, we aim to respond to all queries as quickly as possible by directly providing information to the enquirer or directing them to relevant guidance or information available in the public domain.

IAU Transformation Process

In order to provide a more effective and responsive information and complaint-assessment service, the DPC's IAU has been undergoing a transformation process. Not only have staff numbers in the unit grown from 13 to over 20 in 2018, but also the unit was engaged in a process of restructuring and streamlining of its processes, with a view to providing an enhanced service to the public. In particular, between 25 May and 31 December 2018, work in the unit focused on putting in place new strategies for identifying and responding appropriately to complaints and queries of differing levels of complexity. Enhancing the quality and responsiveness of the service provided by the IAU will continue to be a priority in 2019.

Emerging Trends and Patterns Post-GDPR

The IAU, through analysis of the issues brought to its attention, also identifies emerging trends and patterns of data protection issues that are of concern to individuals and organisations. This helps the DPC to focus its external communications on the most pertinent issues. For example, a notable increase in queries and complaints relating to the use of CCTV, dashcams and bodycams was identified by the IAU in 2018 and specific guidance on this topic was subsequently published by the DPC. Such analysis and learning will continue to help guide the DPC's communications throughout 2019.

The complexity of the queries and complaints received has increased post-GDPR. An increased awareness among the general public of the GDPR and data protection issues is noted, which is likely attributable, at least in part, to the high public profile afforded to data protection matters both pre- and post-GDPR throughout the year. Concurrently, the IAU's interactions with data controllers and processors since the application of the GDPR indicate generally that those organisations continue to make concerted efforts to come to terms with their enhanced obligations under the new regulatory framework.

6 Special Investigations

The DPC's Special Investigations Unit (SIU) was established in 2015 primarily to carry out investigatory work on its own initiative, as distinct from conducting complaints-based investigations. The SIU is proactive in responding to live issues that come to the DPC's attention through a range of channels including the DPC's analysis of trends emerging from performing its complaint-handling functions, issues in the media and concerns raised by civil society, including public representatives and privacy advocates among others. As described earlier in this report, the Data Protection Act 2018 provides for two different types of statutory inquiry — complaint-based inquiries and inquiries of the DPC's own volition as well as audits. Going forward, the focus of the SIU's work will be carried out through own-volition inquiries.

The Public Services Card (PSC)

Work continued between 25 May and 31 December 2018 on the DPC's special investigation of the PSC and its registration process. This investigation began in October 2017 under the Data Protection Acts 1988 and 2003 (as discussed in the 2017 annual report) and must be concluded under that legislation. As referenced in the first annual report for 2018 (Final Report of the Data Protection Commissioner), the purposes of this investigation include:

- to establish if there is a legal basis for processing data in connection with the PSC;
- to examine whether there are appropriate security measures employed in relation to the personal data processed in relation to the PSC;
- to evaluate the information that has been made available to the public; and
- to establish whether this meets the transparency requirements of data protection legislation.

This is a highly complex investigation involving specialist staff from the DPC's investigations, technology and legal divisions that has, to date, involved the examination of a huge volume of material across a range of government sectors, both publicly available and by way of submissions made to the DPC by the data controller, the Department of Employment and Social Protection (DEASP). As referenced in the first annual report for 2018, a draft (138 page) report was issued to the DEASP for comment in August 2018. This contained 13 provisional findings as well as 17 requests for further information. Submissions and further information were received from the DEASP in response to the draft report in late 2018. The DPC's examination of the extensive submissions and materials from the DEASP (comprising some 470 pages) is ongoing.

Surveillance by the State Sector for Law Enforcement Purposes

In June 2018, the DPC, through the SIU, opened 31 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, automatic number-plate recognition (ANPR) enabled systems, drones and other technologies. The use of such technologies for surveillance purposes by the state sector in the conduct of its law-enforcement functions has become prevalent and is perceived by many as an accepted consequence of life in the digital age. In short, 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.

Section 110 of the Data Protection Act 2018 provides for a DPC inquiry into whether infringements of the GDPR are ongoing or have occurred, while Section 123 provides for an equivalent inquiry to be conducted in relation to provisions of the LED, as transposed under the Data Protection Act 2018 (see section on the Law Enforcement Directive for more detail). These own-volition inquiries are being conducted under Section 110 and Section 123 and have been split into a number of modules.

The first module focuses on the 31 local authorities in Ireland, and the second on An Garda Síochána. Further modules are likely to be added as the inquiries progress.

The first and second modules commenced 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 began with a series of on-site inspections in September 2018. From September to December 2018, the SIU carried out 10 on-site inspections in the local-authority sector.

One of the many aspects of these inquiries involves auditing the deployment of community-based CCTV systems by examining whether Section 38 of the Garda Síochána Act 2005 (which provides a legislative basis for such schemes under certain conditions) is being fully complied with, in particular whether the Garda Commissioner has approved all such schemes in operation at present and whether and how the data controller obligations are being met by the local authorities as required under that Act. (A small number of schemes are operated directly by An Garda Síochána, which in those instances acts as data controller.) Linked automatic number-plate recognition is becoming an increasingly prevalent part of these schemes and these inquiries are also examining the basis for this type of surveillance.

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 will also examine the legal basis underpinning the use of these surveillance technologies for law-enforcement purposes. These are important and wide-ranging inquiries and the DPC will continue to prioritise their progression over the course of 2019.

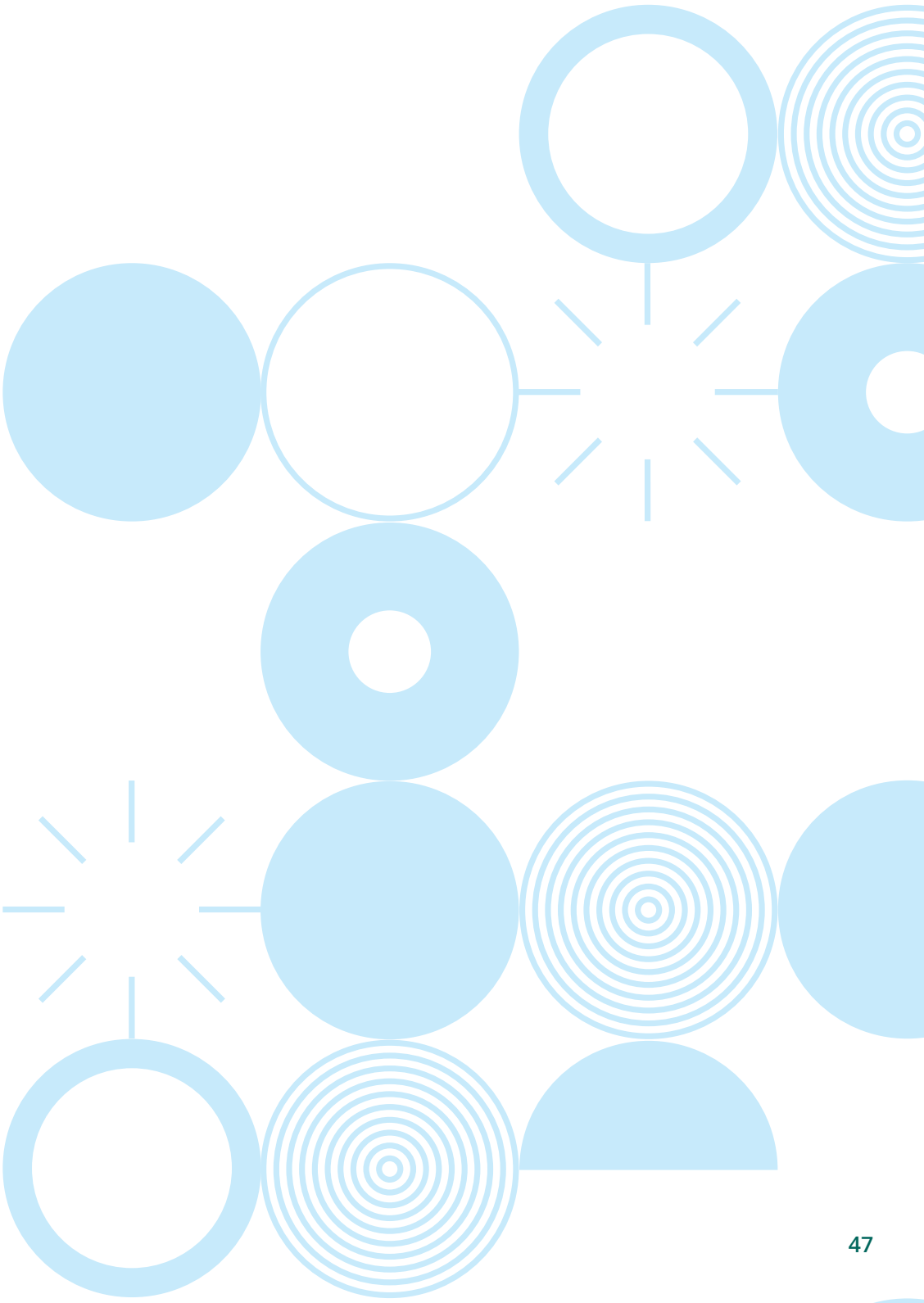
The following two inquiries were initiated by the DPC between 25 May and 31 December 2018:

Inquiry under the Data Protection Act 2018 into data breaches occurring in Tusla. This own volition inquiry under Section 110 of the Data Protection Act 2018 is inquiring into the large volume of data breaches which occurred many of which involved special categories of personal data as defined in Article 9 of the GDPR and the inquiry will look at whether appropriate organisational and technical measures are being implemented by Tusla under the GDPR.

Inquiry under the Data Protection Act 2018 of allegations of infringement of Article 38 (Data Protection Officer) of the GDPR by the Department of Employment Affairs and Social Protection. This inquiry, which is an own volition inquiry under Section 110 of the Data Protection Act 2018, is ongoing.

Another investigation to note:

The DPC investigation of Independent News and Media under the Data Protection Acts 1988 & 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 was ongoing as at 31 December 2018.



7 Technology Multinationals Supervision

The DPC's role in supervising the data-processing operations of the numerous large data-rich multinational companies — including technology internet and social media companies — with EU headquarters located in Ireland changed immeasurably on 25 May 2018. For many, including Apple, Facebook, Microsoft, Twitter, Dropbox, Airbnb, LinkedIn, Oath, WhatsApp, MTCH Technology and Yelp, the DPC acts as lead supervisory authority under the GDPR OSS facility (see the explanation of this principle in the Complaints section of this report). This means that organisations for whom the DPC acts as lead supervisory authority can benefit from having a single point-of-contact with the DPC as a data protection supervisory authority despite being active in more than one EU member state. The role places an important duty on the DPC to safeguard the data protection rights of hundreds of millions of individuals across the EU, a duty that the GDPR requires the DPC to fulfil in cooperation with other supervisory authorities.

Since the implementation of the GDPR, the work and focus of the DPC in the multinational technology sector has been primarily driven by the significant operational demands arising from the OSS and the necessary cooperation and engagement with other supervisory authorities.

The first manifestation of the DPC's greatly expanded role under the GDPR was the complaints lodged on and shortly after 25 May 2018 with supervisory authorities in Belgium, Austria and Germany by NOYB — European Center for Digital Rights and La Quadrature du Net. NOYB and La Quadrature du Net are both not-for-profit associations that represent individuals who believe their data protection rights have been infringed. The GDPR and the Data Protection Act 2018 (which gives further effect to the GDPR) recognise the right of individuals to authorise a not-for-profit body with data protection objectives to lodge a complaint with a DPA on their behalf. As these complaints concerned organisations for which the DPC acts as lead supervisory authority, the complaints were transferred from the relevant authorities with which they were lodged to the DPC. These complaints raised fundamental issues of data protection law compliance and the DPC commenced statutory inquiries to examine whether the organisations concerned are complying with their obligations under the GDPR. Further information is set out in the table below.

The DPC's significantly increased workload relating to the multinational technology sector is further apparent in the following statistics applicable to the period of 25 May to 31 December 2018:

- 260 complaints progressed to complaint-handling processes, including complaints transferred by other EU supervisory authorities, in respect of over 40 organisations.
- 15 statutory inquiries commenced.
- 38 cross-border processing personal-data breach notifications handled, involving 11 organisations.
- 23 formal requests issued by the DPC to organisations under the DPC's general supervision powers seeking detailed information on compliance with various aspects of the GDPR.
- 16 mutual assistance requests (formal and voluntary) received and handled by the DPC from other EU supervisory authorities.

Statutory Inquiries

As of 31 December 2018, the DPC had 15 statutory inquiries (investigations) open in relation to multinational technology companies compliance with the GDPR. Each of these inquiries is being progressed by the DPC pursuant to Section 110 of the Data Protection Act 2018 and, where the inquiry relates to cross-border processing in accordance with, the Cooperation and Consistency Mechanism under Chapter VII of the GDPR.

The inquiries were commenced:

- in response to complaints received by the DPC;
- in response to breaches notified to the DPC; and
- at the DPC's own volition having identified matters that warranted further examination.

Multinational Technology Companies Statutory Inquiries commenced 25 May — 31 December 2018

Company	Inquiry origin	Issues being examined
Facebook Ireland Limited	Complaint-based inquiry	*Right of Access and Data Portability.* 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.
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.
Facebook Ireland Limited	Complaint-based inquiry	*Lawful basis for processing in relation to Facebook's Terms of Service and Data Policy.* 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.
WhatsApp Ireland Limited	Complaint-based inquiry	*Lawful basis for processing in relation to WhatsApp's Terms of Service and Privacy Policy.* 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.
Instagram (Facebook Ireland Limited)	Complaint-based inquiry	*Lawful basis for processing in relation to Instagram's Terms of Use and Data Policy.* 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.
LinkedIn Ireland Unlimited Company	Complaint-based inquiry	*Lawful basis for processing.* 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.
Facebook Ireland Limited	Complaint-based inquiry	*Lawful basis for processing.* 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.
Apple Distribution International	Complaint-based inquiry	*Lawful basis for processing.* 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.

Company	Inquiry origin	Issues being examined
Apple Distribution International	Complaint-based inquiry	*Transparency.* 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.
WhatsApp Ireland Limited	Own-volition inquiry	*Transparency.* 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.
Facebook Ireland Limited	Own-volition inquiry	*Facebook September 2018 token breach.* 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	*Facebook September 2018 token breach.* Examining Facebook's compliance with the GDPR's breach notification obligations.
Facebook Inc.	Own-volition inquiry	*Facebook September 2018 token breach.* 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	*Commenced in response to large number of breaches notified to the DPC during the period since 25 May 2018 (separate to the token breach).* Examining whether Facebook 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 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.

Supervision and Engagement

Under the DPC's general supervision powers, and separate to complaint-handling and inquiry processes, the DPC continued to place significant emphasis on proactive engagement with multinational companies operating in the technology sector between 25 May 2018 and 31 December 2018.

In line with Article 57 of the GDPR, the objective of the DPC's supervision function includes promoting regulatory stability through increasing awareness of controllers and processors of their data protection obligations as well as monitoring relevant developments in information and communication technologies and commercial practices, insofar as they have an impact on the protection of personal data.

Proactive engagement with technology companies enables the DPC to better understand the ways in which personal data are being processed by these companies and the actions they have taken to meet their data protection obligations. This approach further facilitates the DPC in proactively identifying data protection concerns and, in the case of new products or services, ensuring companies are aware of compliance obligations and potential problems in advance of the processing of personal data.

As well as raising awareness and providing guidance, this engagement often results in companies being motivated to adopt measures in response to concerns raised by DPC such as, for example, implementing higher standards of transparency in compliance with the GDPR or reassessing proposals to build in a stronger focus on data protection by design and default. If, following this engagement, there are significant concerns that the company cannot or is unwilling to adequately resolve, the matter can be escalated to a formal DPC inquiry.

Since 25 May 2018, the DPC has engaged with multinational technology companies on a broad range of issues. Examples include:

- Google on the processing of location data.
- Facebook on issues such as the transfer of personal data from third-party apps to Facebook and Facebook's collaboration with external researchers.
- Microsoft on the processing of telemetry data collected by its Office product.
- WhatsApp on matters relating to the sharing of personal data with other Facebook companies.

Supervision engagement with these companies on the matters outlined is ongoing.

The DPC issued 23 formal requests seeking detailed information on compliance with various aspects of the GDPR between 25 May and 31 December 2018.

CASE STUDY 14
'Mentions in the news' feature
(Applicable law — GDPR & Data Protection Act 2018)

In 2018, the DPC received two complaints about a feature on a professional networking platform (the data controller), whereby the data controller sends emails and notifications to a member's connections and followers to inform them if and when the member is mentioned in the news.

The complaints, one of which was lodged with the DPC in March 2018, pre the application of the GDPR and the second of which was received by the DPC in October 2018, arose as a result of the data controller incorrectly associating members with media articles that were not about them. In one of the complaints, a media article that set out details of the private life and unsuccessful career of a person of the same name as the complainant was circulated to the complainant's connections and followers by the data controller. The complainant raised the matter with the data controller and, when it was not resolved to their satisfaction, brought the complaint to the DPC. The complainant stated that the article had been detrimental to their professional standing and had resulted in the loss of contracts for their business. The second complaint involved the circulation of an article that the complainant believed could be detrimental to future career prospects, which the data controller had not vetted correctly.

The key concern arising from these complaints was the failure of the data controller to correctly identify matches between members and those referenced in specific third-party media articles, resulting in members being associated with new stories that were not about them. It was clear from the complaints that matching by name only was insufficient, giving rise to data protection concerns, primarily the lawfulness, fairness and accuracy of the personal data processing utilised by the 'Mentions in the news' feature.

As a result of these complaints and the intervention of the DPC, the data controller undertook a review of the feature. The result of this review was to suspend the feature for EU-based members, pending improvements to safeguard its members' data.

Prior Consultation Under Article 36(1) GDPR

As detailed below in the section on Consultations, a formal mechanism is available to data controllers under Article 36(1) of the GDPR for prior consultation with the DPC in circumstances where the organisation, having undertaken a Data Protection Impact Assessment (DPIA) on a new processing operation, has identified a high risk to the rights and freedoms of individuals that cannot be mitigated. There were no requests to the Technology & Multinationals division under Article 36 for prior consultation in the period of 25 May 2018 to 31 December 2018.

Ad Tech Sector

Since 25 May 2018, the DPC has received several submissions from individuals and privacy advocates concerning the conduct of technology companies in the online advertising sector. Particular focus has been placed on 'behavioural advertising', which utilises personal data gathered from users' online activity in order to serve advertisements that are considered relevant to that person's circumstances. The use of personal data in this manner has caused concern on several grounds, including the following, which were reported to the DPC:

- Profiling of individuals, particularly where special categories of data are involved.
- How location data are being utilised by advertisers.
- Personal data processed for the purpose of advertising a product or service to an individual without a lawful basis.
- Individuals not being aware of parties who have access to their personal data.

The online advertising ecosystem is complex, with a multitude of parties involved in high-speed, voluminous transactions around bidding for advertising space and delivering advertising content. The current model of free internet services and platforms is predicated on the ability of the companies providing those services to derive revenue from offering advertising space. However, the protection of personal data is a prerequisite to the processing of any personal data within this ecosystem and ultimately the sector must comply with the standards set down by the GDPR.

In 2018, the DPC engaged with several stakeholders, including publishers and data brokers on one side, and privacy advocates and affected individuals on the other. The DPC's examination of the sector will continue to be prioritised in 2019, in cooperation with its counterparts at EU level so as to ensure a consistent approach across all EU member states. Furthermore, some of the DPC's statutory inquiries referenced above will conclude this year and contribute to answering some of the questions relating to this complex area.

Mutual Assistance

The GDPR provides for a harmonious approach to the interpretation and implementation of the new legal framework by EU data protection supervisory authorities through various cooperation and consistency mechanisms set out in Chapter VII of the GDPR, one of which is the making of a request for mutual assistance under Article 61 of the GDPR. In 2018, in relation to the multinational technology sector, the DPC received 16 requests — formal and voluntary — for mutual assistance from other EU data protection authorities. The topics that arose include the following:

- transparency of processing agreements and privacy notices;
- the interaction of the GDPR and the ePrivacy Directive; and
- digital advertising in the Ad Tech sector.

8 Technology Leadership

In late 2018, the DPC established an advanced technology evaluation and assessment unit (the Technology Leadership Unit — TLU) with the objective of supporting and maximising the effectiveness of the DPC's supervision and enforcement teams in assessing risks relating to the dynamics of complex systems and technology. The unit is also tasked with drafting and communicating guidance to organisations and individuals on technology and data protection. The DPC has recruited staff with the necessary specialist skills and expertise and continues to build on the unit's capacity through learning and development.

The goal of the DPC in establishing this capability is to confidently and comprehensively promote and raise controller and processor compliance with the GDPR where technology solutions are implemented and where data subject rights are put into effect digitally.

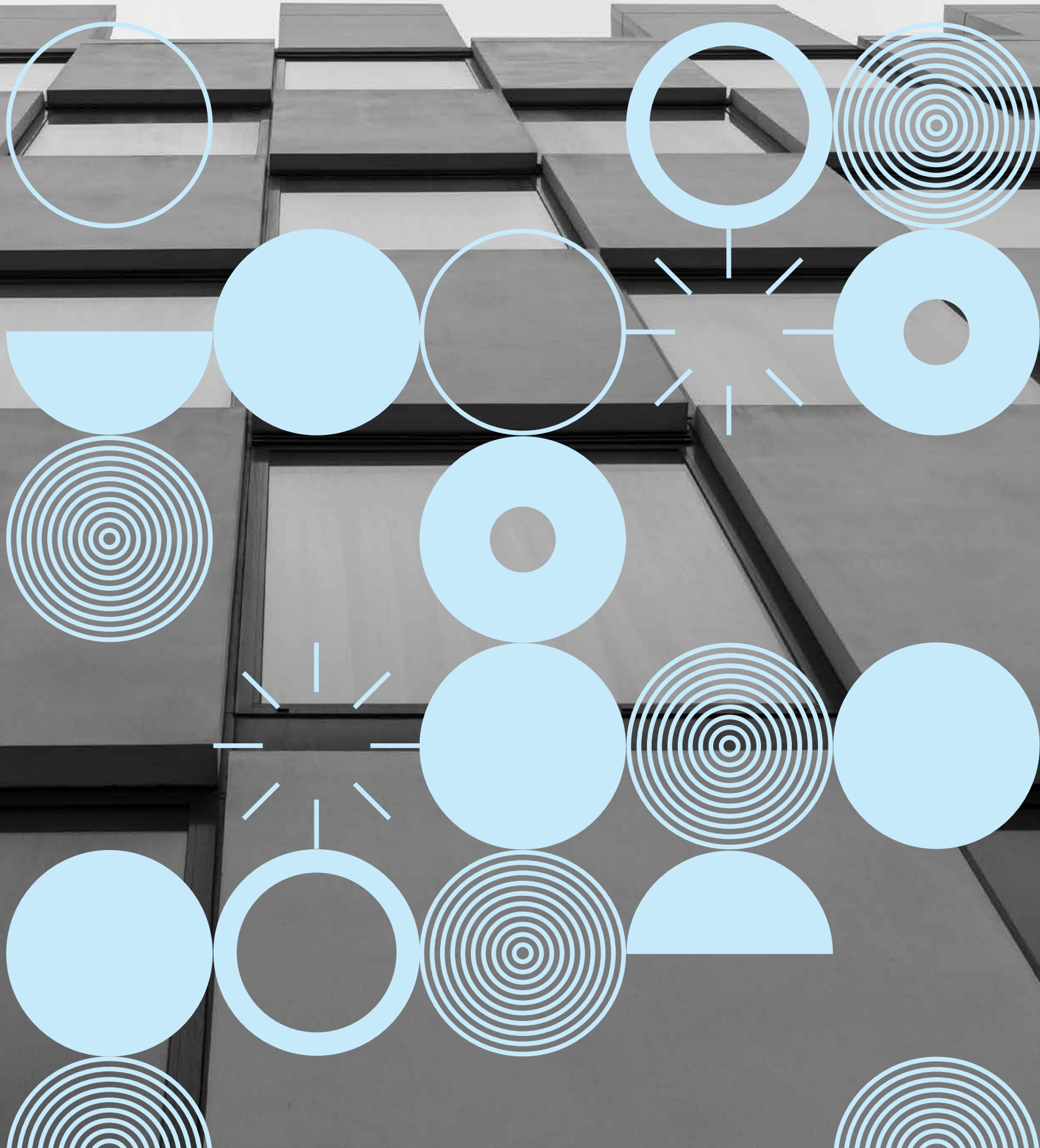
The TLU provides expertise on advanced technology topics through research, monitoring, and analysis. It will provide additional and specialised capability to assist and contribute to inquiries and investigations that involve complex technology elements.

The Unit is building capacity to undertake studies and experimental analysis on the technology based activities, practices and implementation of products by data controllers and processors and to explore a means to engage with them on innovation in the context of regulatory compliance.

Since its establishment, the TLU has enabled the DPC to provide enhanced technology-focused internal guidance on ePrivacy, internet protocols and data portability, advertising technology and accountability. The Unit is planning to provide external guidance, training and outreach in areas such as AI and machine learning, advertising technology, device ID settings and cybersecurity. The TLU expanded the contributions of the DPC to the European Data Protection Board on regulatory opinions pertaining to technology concerns (accreditation and certification, data protection by design, data protection impact assessment) between 25 May and 31 December 2018.

Throughout 2019, the TLU will undertake a range of specific activities to further support the strategic goals and objectives of the DPC. These activities will take the form of "sweeps" or data controller surveys that will inform the DPC of compliance activities; desktop studies evaluating data subjects' perspectives of data controller compliance efforts; and research into contemporary matters such as artificial intelligence and machine learning, encryption, digital ledger technology, digital assistants and identity management and authentication technologies. The TLU aims to progress relationships with technology and innovation teams in other EU and international supervisory authorities; harness experts in academia, standards bodies, professional and sectoral groups, and develop specialised working relationships with other regulatory agencies and external resources.

9 Consultations



The DPC's consultation function plays a pivotal role in advancing a better understanding and awareness of data protection obligations. Through active and meaningful engagement with both public and private sector organisations, the DPC delivers on its remit to drive data controllers' and processors' awareness and understanding of their responsibilities to be compliant with data protection legislation, ensuring that protection of this fundamental right is at the forefront of any project involving the processing of personal data. Taking a strategic approach to our engagement with organisations, in 2018 the DPC continued to focus on proposed data processing projects and initiatives that posed a high risk to the data protection rights of individuals. By providing clear guidance and advice to all organisations on their compliance obligations, the DPC's proactive consultation work continued to deliver results in protecting the public from poor data handling practices by both public and private sector bodies.

General Queries between 25 May and 31 December 2018

The Consultation Unit received 958 general queries during this period (note: these figures do not include consultations with multinational technology companies). The breakdown of the general consultation queries shows slight differences from the trends identified in the final report of the Data Protection Commissioner covering the period from 1 January to 24 May 2018 where over half of queries received came from the private sector. There was an 8% decrease in requests from the private sector, 7% increase in the public sector whereas the health sector remain relatively stable increasing by just 1%. The changes are significant in the sense that traditionally the percentage of requests per sector are generally very stable. The changes would appear to indicate that the public sector is becoming more aware of their data protection responsibilities and their growing engagement with the DPC is very welcome.

1 January — 24 May 2018	%	25 May — 31 December 2018	%	% Change
Health Sector	14%	Health Sector	15%	+1%
Private and Financial	58%	Private and Financial	50%	-8%
Public Sector	28%	Public Sector	35%	+7%

Engagement

The Consultation Unit engaged with numerous stakeholders following the application of the GDPR and the enactment of the Data Protection Act 2018, which transposed the LED and gave further effect to the GDPR in Irish law on 25 May 2018.

Proactive Engagement

The Consultation Unit continued to implement a collaborative stakeholder-led approach to engagement. From a strategic perspective, it is the intention to continue to encourage the development of DPO networks whereby groups of DPOs in a related area collaborate to share knowledge and experience. The unit is open to attending regular roundtable forums with DPO networks and groupings to reflect upon and advise on sector-specific data protection issues. This collaborative approach will ensure that best practices become commonplace and will utilise the resources of the Consultation Unit more effectively. This will also help the unit to identify areas and upcoming trends where specific guidance will be most beneficial.

Data controllers and processors will still be able to seek assistance and guidance from the DPC's Consultation Unit. The new DPC website provides a dedicated portal to submit consultation queries.

DPIA

The requirement to carry out a DPIA is mandatory under certain conditions as prescribed by the GDPR, particularly where a data processing using new technologies is likely to result in a high risk to the rights and freedoms of individuals. A non-exhaustive list specifying the types of processing operations subject to the requirement for a DPIA is available on the DPC website: www.dataprotection.ie.

Guidance materials are also available on the DPC website to assist data controllers in:

- determining whether they need to carry out a DPIA; and
- identifying the steps required to carry out a DPIA.

Mandatory consultation in respect of DPIAs is only necessary when the processing would result in a high risk in the absence of measures taken to mitigate the risk. The Consultation Unit will continue to provide general assistance to controllers in respect of their responsibilities regarding conducting DPIAs.

Prior Consultation and Legislative/ Regulatory Measures

Providing legislative observations has become a key role of the DPC's consultation function following the application of the GDPR and the enactment of the Data Protection Act 2018. Since 25 May, under the statutory prior-consultation provisions in the Data Protection Act 2018, the DPC has been formally consulted on three key pieces of secondary legislation seeking either to restrict the rights of data subjects or to specify suitable and specific measures for processing in accordance with the GDPR and the Data Protection Act 2018 (details beneath). It is anticipated that this function will grow substantially in 2019.

More broadly, the GDPR provides for mandatory consultation with data protection supervisory authorities on all legislative and regulatory proposals. It is important that bodies involved in drafting legislative proposals or regulatory measures consult directly with the DPC before further steps are taken to advance the legislative proposal or regulatory measure. Article 36(4) of the GDPR and various sections of the Data Protection Act 2018 set out further provisions regarding this prior-consultation requirement. Webforms are also available on the DPC website to assist with making a request of this nature.

The prior-consultation requirement is not a tick-box exercise. The relevant body should carry out the appropriate level of assessment and provide an evidence-based rationale to underpin their draft proposal(s) in advance of seeking a consultation with the DPC. This will also help to accelerate the consultation process and perhaps even deliver a more positive outcome for the body concerned.

In the period between 25 May and31 December 2018, the DPC engaged with various stakeholders on several legislative matters including those outlined below.

Statutory prior consultation under the Data Protection Act 2018 — no significant concerns raised by the DPC

- Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018[3]
- Data Protection Act 2018 (Section 60(6)) (Private Security Services Act 2004, Property Services (Regulation) Act 2011 and Personal Insolvency Act 2012) Regulations 2018[4]
- Data Protection Act 2018 (section 60(6))(Central Bank of Ireland) Regulations 2018[5]

3 Specification of suitable and specific measures for processing under section 36(2) Data Protection Act 2018

4 Restriction of data subject rights in accordance with Article 23 GDPR and section 60 Data Protection Act 2018

5 Restriction of data subject rights in accordance with Article 23 GDPR and section 60 Data Protection Act 2018

Sample of Ongoing Legislative Consultations

- Child Care (Amendment) Bill 2018
- Patient Safety Bill 2018
- Irish Human Rights (Gender Pay Gap Information) Bill 2018
- Health Insurance (Amendment) Bill 2018
- Credit Union Restructuring Board (Dissolution) Bill 2018
- Local Government Bill 2018 (Cork County Council)
- Animal Health and Welfare Act 2013 (Surveillance)
- Residential Tenancies Amendment Bill 2018
- Judicial Council Bill 2017
- Retention of Records Bill 2018
- Draft Memorandum for the Government: Road Traffic (Miscellaneous Provisions) Bill 2018/General Scheme of a Road Traffic (Miscellaneous Provisions) Bill
- Data Sharing and Governance Bill 2018
- Defence Forces Evidence Bill 2018
- Adoption (Information and Tracing Bill) 2016
- Draft Memorandum for the Government: Regulated Professions (Health and Social Care) (Amendment) Bill 2018
- Criminal Records (Exchange of Information) Bill 2018
- Regulation of the European Parliament and of the Council amending Regulation (EU,Euratom) No 1141/2014

Below is a list of some of the organisations and projects/ strategies that the DPC Consultation Unit engaged with between 25 May and 31 December 2018.

Public

- The ESB and the roll out of Smart Metering (ongoing)
- Department of Foreign Affairs/Passport Office and the online passport adult renewal system
- Department of Expenditure and Reform — Public Service Data Strategy 2018 — 2021
- Department of An Taoiseach — Regulation of Online Political Advertising
- Financial Services and Pensions Ombudsman and their GDPR readiness programme.
- Various public sector entities and bodies representing elected representatives in relation to guidance on canvassing for electoral purposes, public representations and constituency office best practices.
- TUSLA/Department of Children and Youth Affairs and an Garda Síochána– reporting child welfare concerns (ongoing)

Health

- Department of Health and the Health Research Board — Health Research Regulations.
- HIQA — Standard for Public Consultation: Information Requirements for a National Patient Summary
- HIQA — Recommendations for a National, Community-based ePrescribing programme for Ireland
- Mental Health Commission and the Assisted Capacity Decision Act 2015.

Voluntary

- Disability Federation Ireland (DFI) — presentation at annual meeting.
- Interactive workshop to The Wheel's DPO network which was attended by over 60 key data protection staff from a wide range of community and voluntary organisations.

Private and Financial

- Engagement continued with representative groups such as BPFI, Insurance Ireland, Retail Excellence, National Recruitment Federation, Brokers Ireland, Accountancy Ireland, TIF, Credit Unions Compliance Centre, Pensions sector (IAPF), banks and insurance companies, on issues that ranged from compliance with the GDPR, to potential Codes of Conduct and possible consequences of Brexit.
- Companies Registration Office (CRO) and the Departments of Finance and Business, Enterprise & Innovation on the creation of a database for the purpose of complying with Article 30 (3) of EU Directive 2015/849 (the 4th AML Directive).

Law Enforcement

- Director of Public Prosecutions — Application of the Law Enforcement Directive/Part 5 Data Protection Act 2018 and transfers of data
- Policing Authority and Statement of Strategy/ Priorities
- Defence Forces and GDPR/Law Enforcement Directive readiness project
- An Garda Síochána — GDPR preparations

Consultation 2019 — What to Expect?

The consultation unit has recently been expanded and re-structured into three new dedicated teams, each headed by an Assistant Commissioner:

- Public Sector and Law Enforcement
- Health and Voluntary Sector
- Private and Financial,

This restructuring will improve the consultation function, extend the DPC's reach, facilitate the development of more sector-specific guidance, and develop additional awareness-raising approaches in key areas across all sectors at European and domestic levels.

Public Sector and Law Enforcement

The Public Sector and Law Enforcement team will continue to consult in relation to legislative proposals involving the processing of personal data. Another area of high priority is the local-authority sector; the team is committed to producing further guidance in 2019.

The team will also prioritise engagement with law-enforcement processing activities, the LED and Part 5 of the Data Protection Act that transposes the directive into Irish law. It is important for all bodies with law-enforcement power to correctly identify cases in which the legal regime of the LED and Part 5 of the Data Protection Act 2018 applies. There is effectively a two-step test to determine whether the processing in question is within the scope of the LED and Part 5 of the Act:

- First, the data controller responsible for the processing in question must be a 'competent authority' as defined by Section 69 of the Act.
- Second, the processing in question must be for 'law enforcement purposes', as defined in Section 70 of the Act.

In 2019, the DPC intends to meet with as many relevant organisations (and sub-units) as possible to discuss their responsibilities under the legislation. Relevant bodies and their DPOs are invited to contact the DPC and assist in identifying and mapping out guidance materials that would be beneficial to the sector.

Health and Voluntary

It is important that patients have confidence in the health services they need to access, often under difficult personal circumstances. This extends to confidence in how their personal data is processed. The Health and Voluntary Consultation team will continue to engage with all stakeholders in the health sector to promote data protection best practice. This will include engagement with government, health providers in the public and private spheres, health researchers, patient organisations and the Medtech sector to proactively address challenges that arise. The Health Consultation team will also contribute to the work of the Compliance, eGovernment and Health Expert Subgroup of the EDPB.

This new consultation team is also tasked with providing guidance to data controllers in the charity and voluntary sector. Following on from the positive feedback received from engagement with the sector in 2018, the DPC will continue to update and develop sector-specific guidance. The DPC has targeted key network actors and engagement that to date has helped identify the most challenging data protection queries charities and volunteer groups are seeking guidance on. The DPC plans to issue targeted guidance for the charity sector in the second and third quarters of 2019.

Private and Financial

The GDPR and DPC engagement with the private and financial sector in 2018 contributed to significantly greater awareness of data protection obligations, with many companies post-25 May continuing to update data protection policies and procedures, provide staff training, and invest in new IT systems and support for the DPO role within their organisations. While many companies take their compliance responsibilities under the GDPR very seriously, challenges remain, in particular the presentation and readability of customer notices and privacy policies in compliance with transparency standards set by the GDPR. In 2019, the DPC will continue to engage with companies on transparency standards. Other priorities for the sector will include engagement with the financial and insurance sectors to better understand the application of emerging technologies to their data-processing operations, and the ongoing monitoring, including statutory consultation where required, of proposals to implement national banking and insurance fraud databases.

10 Legal Affairs

Overview

The DPC's Legal Unit operates horizontally within the DPC and is responsible for legal oversight and the provision of internal legal advice and support across all of the DPC's functions, and in respect of all litigation in which the DPC is involved. The Legal Unit also provides training on a rolling basis to all staff within the organisation on a wide range of issues including the applicable legal frameworks, legal developments and the performance of the DPC's functions at national and EU levels. In addition to the centralised Legal Unit, the DPC employs other staff with legal qualifications.

The expansion of the DPC's Legal Unit continued between 25 May and 31 December 2018. Several specialist legal advisors joined the unit, significantly increasing the capacity of the DPC's internal legal advisory and support resources.

Additionally, the Legal Unit now also encompasses policy development. Specialist senior policy officers, appointed in the areas of Children's Policy, and Guidance & Policy Development, report to the Deputy Commissioner (Head of Legal).

On the DPC's new website — www.dataprotection.ie — launched in December 2018, a dedicated tab for legal developments provides information on the applicable legislative frameworks governing data protection, as well as details of relevant judgments in cases involving the DPC.

Prosecutions by the DPC

Prosecutions were taken by the DPC between 25 May and 31 December 2018 under the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011) (also known as the e-Privacy Regulations).

Five entities were prosecuted for offences under Regulation 13 of S.I. No. 336 of 2011 in respect of electronic direct marketing. The summonses for these five cases covered a total of 30 offences. Prosecution case studies are set out below.

Prosecutions Case Studies

CASE STUDY 15
Prosecution of Viking Direct (Ireland) Limited

In April 2017, we received a complaint from a business owner regarding unsolicited marketing emails that the business email address was receiving from Viking Direct (Ireland) Limited. The complainant indicated that she had previously contacted the company to ask for her business email address to be removed from the marketing list but, despite this, further marketing emails continued to be sent.

During our investigation, Viking Direct (Ireland) Limited confirmed that the complainant had asked to be removed from its mailing list several times. It explained that the internal processes of moving the data to the suppression list had failed and the data remained on the mailing list. The company stated that the systems had now been corrected and tested, such that the situation should not recur. It apologised for any inconvenience caused to the complainant. Our investigation found evidence of three opt-out requests sent by the complainant to Viking Direct (Ireland) Limited by email between 30 March 2017 and 11 April 2017.

Viking Direct (Ireland) Limited had been the subject of an investigation in 2012 on foot of a complaint made to the DPC about unsolicited marketing emails. At that time, we concluded that investigation with a warning to the company. In light of that warning, the DPC decided to prosecute the company in respect of the 2017 complaint.

At Dublin Metropolitan District Court on 14 May 2018, the company entered a guilty plea to one charge of sending an unsolicited marketing email to a business email address in contravention of Regulation 13(4) of S.I. No. 336 of 2011. Under this regulation, it is an offence to send an unsolicited direct-marketing communication by electronic mail to a subscriber (which includes business subscribers) where that subscriber has notified the sender that it does not consent to the receipt of such a communication. The case was adjourned for sentencing until 11 June 2018. At the sentencing hearing, the court applied Section 1(1) of the Probation of Offenders Act in lieu of a conviction and fine. The company agreed to cover the prosecution costs incurred by the DPC.

CASE STUDY 16
Prosecution of Clydaville Investments Limited, T/A The Kilkenny Group

In November 2017, we received a complaint from an individual who received a marketing email from the Kilkenny Group. The email, which was personally addressed to him, promoted a pre-Christmas sale and informed him that there was up to 50% off and that everything was reduced. The complainant informed us that he did not believe that he had opted into receiving marketing emails.

During our investigation, it emerged that a previous marketing email had been sent to the same complainant one year earlier, in November 2016, inviting him to a corporate event in the company's Cork store. The complainant subsequently advised us that he recalled replying to that email, asking that his email address be deleted.

In September 2012, arising from our investigation of a complaint about unsolicited marketing text messages sent by the Kilkenny Group to a different complainant, we had issued a warning to the company. In light of that, the DPC decided to prosecute the company in respect of the 2017 complaint.

The matter came before Tralee District Court on 15 October 2018. The defendant faced a total of four charges. Two related to alleged contraventions of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of unsolicited marketing emails to the complainant in November 2016 and November 2017 without his consent. Two further charges related to alleged contraventions of Regulation 13(12)(c) of S.I. No. 336 of 2011. This regulation provides that a person shall not send electronic marketing mail that does not have a valid address to which the recipient may send a request that such a communication shall cease. As guilty pleas were not entered to any of the charges, the matter went to a full hearing involving three defence witnesses and two prosecution witnesses, including the complainant. At the end of the proceedings, the court found the facts were proven in relation to two contraventions of Regulation 13(1) in relation to the sending of two marketing emails without consent. On the understanding that the defendant would discharge the prosecution costs of €1,850, the court applied Section 1(1) of the Probation of Offenders Act in respect of both charges in lieu of a conviction and fine. The court dismissed the two charges in respect of Regulation 13(12)(c).

CASE STUDY 17
Prosecution of DSG Retail Ireland Limited

DSG Retail Ireland Limited operates under various trading names and registered business names such as Dixons, Currys, PC World and Currys PC World. In November 2017, we received a complaint from a woman who had purchased a television from Currys a year previously. She informed us that she gave her email address to the company for the purposes of receiving a receipt and that she did not consent to receiving marketing emails. She stated she had unsubscribed from receiving further emails but the unsolicited emails continued.

During our investigation, the company told us that the customer had successfully unsubscribed from its mailing list in November 2016. However, when she made a new purchase in January 2017 and once again opted out of receiving marketing communications, a duplicate record was created following the customer's second transaction. According to the company, this duplicate record, coupled with a system bug arising during an update to its systems in May 2017, resulted in an error regarding the recording of the customer's marketing preferences. As a result, there was a period between August and November 2017 during which marketing emails were sent to her.

As we had previously issued a warning to the company in November 2014 on foot of a previous complaint from a member of the public concerning an alleged contravention of the regulations in relation to unsolicited marketing emails, the DPC decided to prosecute the company in respect of the latest suspected contravention.

At Dublin Metropolitan District Court on 22 October 2018 the company entered a guilty plea in relation to a charge for contravention of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of an unsolicited marketing email to the complainant without her consent. In lieu of a conviction and fine, the court ordered the company to make a charitable donation of €1,500 to the Peter McVerry Trust. The defendant company agreed to cover the prosecution costs of the DPC. Confirmation of the charitable donation was subsequently provided to the court on 26 November 2018 and the matter was struck out.

CASE STUDY 18
Prosecution of Vodafone Ireland Limited

In May 2018, we received a complaint from an individual who stated he was receiving frequent unsolicited calls from Vodafone's marketing team. He claimed that Vodafone initially called him on 10 May 2018, at which point he said he was not interested in their offer; since then the company had called him every day. He ignored the communications.

During our investigation, we confirmed that a recording of the marketing telephone call on 10 May 2018 included the complainant advising the calling agent that he was not interested in Vodafone's broadband service. Vodafone told us that the agent should have then removed the telephone number from the marketing campaign by using an appropriate code when closing the call. Human error had led to the phone call being closed with an incorrect code for a call-back — meaning the complainant's phone number remained, leading to the further calls.

We received a separate complaint in July 2018 from a Vodafone customer. He reported that he had received an unsolicited marketing telephone call from Vodafone in June 2018 despite having opted out of receiving marketing telephone calls during a previous unsolicited marketing telephone call in May 2018, confirmation of which had been sent to him by email shortly afterwards.

In response to our enquiries, Vodafone referred to a data-breach report that it had submitted to the DPC on 21 June 2018. This report notified the DPC that several customers who had opted out of marketing between 18 May and 11 June 2018 had erroneously received marketing communications due to difficulties in the implementation of system changes as part of its GDPR-compliance programme. This resulted in recently changed marketing preferences not being read clearly on all its systems and, accordingly, the customers concerned were wrongly included in marketing campaigns.

The DPC decided to prosecute Vodafone in relation to both cases. At Dublin Metropolitan District Court on 22 October 2018, the company entered guilty pleas in relation to two charges for contraventions of Regulation 13(6)(a) of S.I. No. 336 of 2011 for the making of unsolicited marketing telephone calls to the mobile telephones of the two complainants without their consent. The court convicted Vodafone on the two charges and imposed fines of €1,000 in respect of each of the two charges (a total fine of €2,000). Vodafone agreed to cover the prosecution costs of the DPC.

CASE STUDY 19
Prosecution of Starrus Eco Holdings Limited, T/A Panda and Greenstar

In April 2018, a customer of the bin-collection service provider, Panda, complained to us that he had received unsolicited marketing SMS and email messages to which he had not consented, advertising Panda's electricity business. He stated that the messages did not provide an unsubscribe option.

During our investigation, we were informed by Panda that the complainant should not have received the marketing messages. It said that due to a human error, a staff member of the marketing department had incorrectly believed that the complainant had consented to receiving direct-marketing messages. It regretted the failure to include an opt-out on the messages and explained that its service provider for marketing emails had failed to act in accordance with its instructions to include an opt-out.

In May 2018, we received a complaint from a customer of Greenstar, another bin-collection service provider. This individual had previously complained to us in 2011 about unsolicited marketing text messages sent to him without consent. We concluded that previous complaint by issuing a warning to Greenstar in September 2011. The complainant now reported to us that direct marketing from Greenstar by means of SMS messages had started aggressively once again.

In response to our enquiries, Greenstar informed us that given the lapse of time (which it acknowledged was absolutely no excuse) since the 2011 complaint, its records pertaining to the complainant were not what they should have been with respect to the complainant having previously opted out of receiving marketing from the company — that neither the complainant's details nor details of the 2011 complaint were accurate and up-to-date, insofar as it should not have used the complainant's mobile telephone number for marketing purposes.

In light of our previous warning, the DPC decided to prosecute Starrus Eco Holdings Limited, T/A Panda and Greenstar in respect of offences committed in both cases. At Dublin Metropolitan District Court on 24 October 2018, the company entered guilty pleas in relation to charges for contraventions of Regulation 13(1) of S.I. No. 336 of 2011 for the sending of unsolicited marketing SMS messages to the two complainants without their consent. In lieu of a conviction and fine, the court ordered to company to make a charitable donation of €2,000 to the Peter McVerry Trust. The defendant company agreed to cover the prosecution costs of the DPC. Confirmation of the charitable donation was subsequently provided to the court on 15 November 2018 and the matter was struck out.

Litigation Involving the DPC

Between 25 May and 31 December 2018, judgments were delivered in the following proceedings to which the DPC was a party. It should be noted that all 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 High Court in the case of Agnieszka Nowak v The Data Protection Commissioner [2018] IEHC 443 (Judgment of the High Court delivered 12 July 2018)

Key issue: compliance with an access request which is specific and limited in its terms.

This case involved an appeal by a data subject to the High Court (heard in June 2018) against the Circuit Court decision from February 2018. In the latter case, the data subject's appeal of the DPC's decision on the appellant's complaint had been dismissed. The data subject's complaint related to an access request that had been made to her employer in which she had sought 'a copy of all documents held [...] which constitute personal data [...] namely [...]' The access request had then gone on to specify three particular categories of documents. The employer had provided the data subject with the stipulated categories of personal data but the data subject later complained to the DPC that not all her personal data had been provided (she provided examples). She also complained that she had not been provided with a description of the personal data and the categories, purposes and recipients of the personal data processed and that, consequently, the employer was in breach of its obligations under Section 4 of the Data Protection Acts 1988 and 2003 (the DPA). The employer maintained that the access request had been limited to the three categories of documents and that the further information which the data subject had later identified as missing from the response to the access request had not been within the scope of the access request. However, it subsequently provided the further personal data. The data subject later confirmed that she had no further issues regarding her access request but requested a formal decision from the DPC.

The DPC's decision was that while Section 4 of the DPA provided a data subject with the right to a copy of any personal data held about them by an organisation, where a data subject explicitly limits their access request, it is legitimate and appropriate for the organisation to solely provide the personal data specified rather than all the personal data held. As such, the DPC found the employer's limitation of its response to the access request to only the three specified categories of personal data to be reasonable and that none of the additional personal data, which had been furnished after the complaint had been made, fell within those categories. On that basis there was no breach of Section 4 of the DPA. The DPC also found, on the basis of its interpretation of the sub-provisions of Section 4, that in specifically requesting a copy of the personal data in question, it was reasonable for the employer to assume that the data subject was not seeking the descriptions of the personal data processed as provided for in Section 4 under a general request. Accordingly, the fact that the employer had not provided the descriptions of the personal data did not constitute a contravention of the DPA.

The judgment of the Circuit Court found that the DPC's conclusion regarding the word 'namely' was entirely reasonable and that the DPC's decision was 'reasoned, rational, lucid and entirely reasonable'. In the High Court's judgment, Mr Justice McDermott found that while pro-

cedural points had been raised in the appeal to the High Court, the essence of the issue raised by the data subject was whether her employer had complied with its legal obligations under the DPA and that this went back to the interpretation of the initial access request. He noted that the data subject's request was 'not a general request', but that she 'clearly knew what she wished to obtain and selected three categories from a wider category of documentation', and when she used the word 'namely' in that request 'she was clearly identifying the documents and could equally have said "that is to say" or "specifically", which have the same meaning'. The High Court was satisfied that the Circuit Court judge did not err in accepting the DPC's position that the access request was not general in nature but was limited to the three categories. The access request was a limited one and not a wide-ranging one engaging all the sub-paragraphs of Section 4(1)(a). It was entirely open to a data subject to make a focused request for data under the DPA but it was not reasonable for a data subject, having made a specific and limited access request, to complain to the DPC about a failure to provide documents that had not been specifically provided. At a minimum, the court said, it should be expected that the data subject should raise the issue with the data controller before complaining to the DPC. The appeal was therefore dismissed.

Note: This High Court decision is now the subject of an appeal to the Court of Appeal.

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 Commissioner commenced proceedings in the Irish High Court seeking a reference to the 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 Commissioner 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–US personal-data transfer regime). The CJEU ruled that this procedure (involving seeking a reference to the CJEU) must be followed by an EU DPA where a complaint that is made by a data subject concerning an EU instrument, such as an EU Commission decision, is considered by the EU DPA to be well founded.

(1) Background

The proceedings taken by the Commissioner have their roots in the original complaint made in June 2013 to the Commissioner about Facebook by Mr Maximillian 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., it could be 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 programs said to be operated by the US National Security Agency, notably PRISM. The (then) Commissioner 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 Commissioner's decision not to investigate his complaint and that action resulted in the Irish High Court making a reference to the CJEU, which in turn delivered its decision on 6 October 2015.

(2) CJEU procedure on complaints concerning EU Commission decisions

The CJEU ruling of 6 October 2015 made it clear that where a complaint is made to an EU DPA which involves a claim that an EU Commission decision is incompatible with protection of privacy and fundamental rights and freedoms, the relevant DPA must examine that complaint even though the DPA itself cannot set aside or disapply that decision. The CJEU ruled that if the DPA considers the complaint to be well founded, then it must engage in legal proceedings before the national court. If the national court shares those doubts as to the validity of the EU Commission decision, it 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 that underpinned the Safe Harbour EU–US data-transfer regime.

(3) Commissioner'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 Commissioner agreed to proceed on the basis of that reformulated complaint. The Commissioner 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 Commissioner 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 Commissioner 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 Commissioner'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 Commissioner 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 Commissioner 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 Commissioner 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 Commissioner's consideration of Mr Schrems' complaint against Facebook Ireland. Both parties chose to participate fully in the proceedings. Ten interested third parties also applied as amicus curiae ('friends of the court') to the proceedings and the court ruled that four of those 10 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 Commissioner, Facebook Ireland and Mr Schrems; and (ii) each of the 'friends of the court' as noted above. The court also heard oral evidence from a total of five expert witnesses on US law, as follows:

- Ms Ashley Gorski, expert witness on behalf of Mr Schrems.
- Professor Neil Richards, expert witness on behalf of the DPC.
- Mr Andrew Serwin, expert witness on behalf of the DPC.
- Professor Peter Swire, expert witness on behalf of Facebook.
- 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), several 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 Commissioner 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 may make a ruling as to the validity of the European Commission decisions that 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 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, among 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' that they alleged had been made in the judgment of 3 October 2017. The court reserved its judgment on these matters.

(6) Questions to be referred to the CJEU

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

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

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

made by the parties in relation to Facebook's application for a stay.

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

(7) Appeal to the Supreme Court

On 11 May 2018, Facebook applied for leave to appeal to the Supreme Court against the judgments delivered by the High Court in favour of the DPC on 3 October 2017 (as revised on 12 April 2018). 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 but leaving open the following questions:

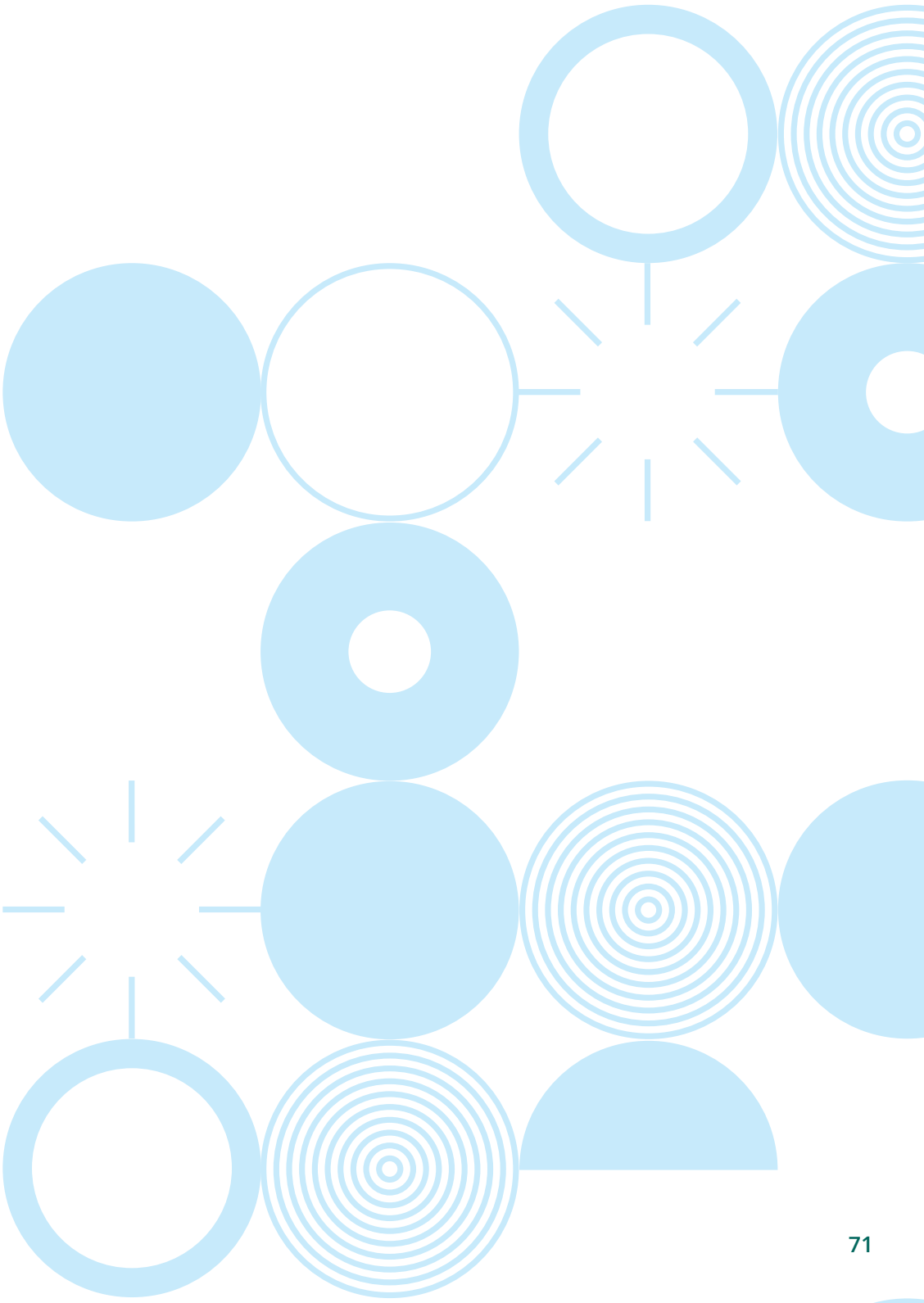
- Does any appeal at all lie against the High Court's judgment?
- If it does, what is the nature of that appeal?

During late 2018, there were several procedural hearings in the Supreme Court in preparation for the hearing of the appeal proper. The substantive hearing of the appeal then took place over 21, 22 and 23 January 2019 before a 5 judge Supreme Court panel composed of Chief Justice Clarke, Mr Justice Charleton, Ms Justice Finlay Geoghegan, Ms Justice Dunne and Mr Justice O'Donnell. Oral arguments were made on behalf of Facebook, the DPC, the US Government and Mr Schrems. Some of the central questions arising from the appeal include the following: can the Supreme Court revisit the facts found by the High Court relating to US law? (This arises from allegations by Facebook and the US Government that the High Court judgment, which underpins the reference made to the CJEU, contains various factual errors concerning US law). If the Supreme Court considers that it may do so, further questions will then arise for the Court as to whether there are in fact errors in the judgment and if so, whether and how these should be addressed. At the time of going to print there is no indication as to when the Supreme Court judgment will be delivered.

In the meantime, the High Court's reference to the CJEU remains valid and is pending before the CJEU.

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.

Data Protection Case Law from the CJEU can be found in Appendix I of this report.



11 Binding Corporate Rules

Binding Corporate Rules (BCRs) were introduced by the EU Article 29 Working Party (now replaced by the EDPB) in 2003, following discussions in response to the need for organisations to have a global approach to data protection because many have several or more subsidiaries located around the globe. As the transfer of data was happening on a large scale, it was recognised that this need must be met in an efficient way to avoid multiple contract signings, e.g. standard contractual clauses or approvals by several DPAs. In Article 47, the GDPR outlines how BCRs can continue to be used as an appropriate safeguard to legitimise transfers to third countries. However, under Article 63, BCR applications are now subject not only to approval by the relevant DPA; in advance of this they must also be considered by the EDPB by way of an opinion issued under the consistency mechanism in Article 64 of the GDPR.

Between 25 May and 31 December 2018, the DPC continued to act, or commenced acting, as lead reviewer in relation to 11 BCR applications. It is expected that the DPC will issue approval decisions on a number of these applications in the first half of 2019 once the EDPB has given its opinion in accordance with the consistency mechanism set out in Article 64 of the GDPR. The DPC has also assisted other DPAs by acting as co-reviewer on eight BCRs in this period.

Between 25 May 2018 and 31 December 2018, the DPC was also contacted by several companies who indicated that they were considering moving their lead authority for BCR purposes from the UK to Ireland in light of Brexit. Consequently, it is possible that the DPC may see an increase during 2019 in respect of BCR applications received.

Other International Tranfers Issues

Staff from the DPC attend meetings of the EDPB International Transfers Expert Subgroup (ITES), which meets regularly to consider, advise and prepare documentation on matters concerning international transfers of personal data. The subgroup advises the EDPB on these issues as necessary. Through its attendance at these meetings between 25 May and 31 December 2018, the DPC was involved in the development of EDPB positions on important issues including:

- assessment and production of an Opinion of the EDPB under Article 70 of the GDPR on the European Commission draft implementing decision on the adequate protection of personal data in Japan (draft adequacy decision under Article 45 GDPR);
- participation in the second annual review on the functioning of the EU–US Privacy Shield with representatives of the European Commission, the US Department of Commerce, the Federal Trade Commission, the US Department of Transportation, the US Office of the Director of National Intelligence, the Acting Ombudsperson and other US representatives. The EDPB follow-up report was drafted with the assistance of the ITES;
- development of guidelines on international transfers between public bodies for administrative cooperation purposes, which will be submitted to the EDPB for adoption in 2019;
- development of guidance on Article 3 of the GDPR, which deals with the territorial scope of the GDPR. The ITES will continue working on this issue in 2019; and
- commencement of work on guidance on the use of Certification and Codes of Conduct as transfer tools, which will continue into 2019.

12 EU and International

In the years leading up to the GDPR, the DPC's regulatory role had become an increasingly prominent one at an EU and global level, given that the European headquarters of many large technology multinationals are in Ireland. Since 25 May, with the introduction of the OSS, the DPC has played a central role in safeguarding and enforcing the data protection rights of millions of individuals across the EU. In 2018, the DPC created a dedicated unit to facilitate cooperation and engagement with other data protection authorities, both under the OSS model and in the wider international context.

EDPB Engagement

The EDPB was established when the GDPR came into effect on 25 May 2018. The functions of the EDPB are significantly augmented from those of the Article 29 Working Party that it effectively replaced, and include oversight of the consistent application of the GDPR. As an EU data protection supervisory authority, the DPC is a member of the EDPB. Between May and December 2018, the DPC actively participated in the work of the EDPB, which involved DPC staff preparing for and attending over 40 in-person meetings in Brussels, and delivering on commitments as lead and co-rapporteur for EDPB guidelines and policy positions.

The EDPB is empowered to issue opinions on particular measures to be adopted by national supervisory authorities to ensure consistent application of the legislation. The DPC was in the first group of supervisory authorities to submit a list of processing operations requiring a DPIA to the EDPB, as required under Article 35(4) of the GDPR. As a member of the EDPB, we participated in the application of the consistency mechanism that resulted in the adoption of 26 separate opinions on DPIA lists between May and December 2018.

DPC staff have contributed to the development of guidelines, working materials and draft procedures across all EDPB expert subgroups:

- Borders, Travel and Law Enforcement
- Cooperation
- Compliance, eGovernment and Health
- Enforcement
- Financial Matters
- Fining Taskforce
- International Transfers
- IT Users
- Key Provisions
- Social Media
- Strategic Advisory
- Technology

In the latter half of 2018, DPC staff continued to take a leadership role as lead rapporteur for the Guidelines for Codes of Conduct, due for adoption by the EDPB in early 2019. We have also contributed as co-rapporteurs on Guidelines on Certification, the EDPB Enforcement strategy, as well as Guidelines on the Interplay between Article 3 (Territorial Scope) and Chapter V of the GDPR during this time. Since being appointed in May 2018, the DPC continued in its role as a co-coordinator for the Social Media Expert subgroup, whose function is to develop guidance and set strategic priorities relating to the processing of personal data by social media companies.

The DPC's Consultation Unit continues to have full representation at the EDPB. It also made significant contributions on behalf of the DPC at all the EDPB Financial and eGovernment subgroup meetings between 25 May and 31 December 2018.

The unit is the lead rapporteur on Code of Conduct Guidelines (which are expected to be published in the first quarter of 2019). Its participation in the Financial Matters Experts subgroup continued with the main areas of focus being on the operation of the Foreign Account Tax Compliance Act (FATCA) and Common Reporting Standard (CRS) in tax authorities across the European member states. We also continue to monitor new developments in the Fintech industry in the use of blockchain, security and big-data processing. Finally, we are assessing the impact of the 'Payments Services Directive', (PSD2) on the banking sector and the applications (apps) that allow third parties to access and deliver payment of services by way of the consent of a customer via his or her bank account.

Social Media Expert Subgroup

The DPC continues to act as co-ordinator of the Social Media Expert Subgroup of the EDPB, and in that context the DPC is acting as lead rapporteur to identify strategic priorities of the subgroup working in tandem with other subgroups, where necessary relating to the processing of personal data by social media companies.

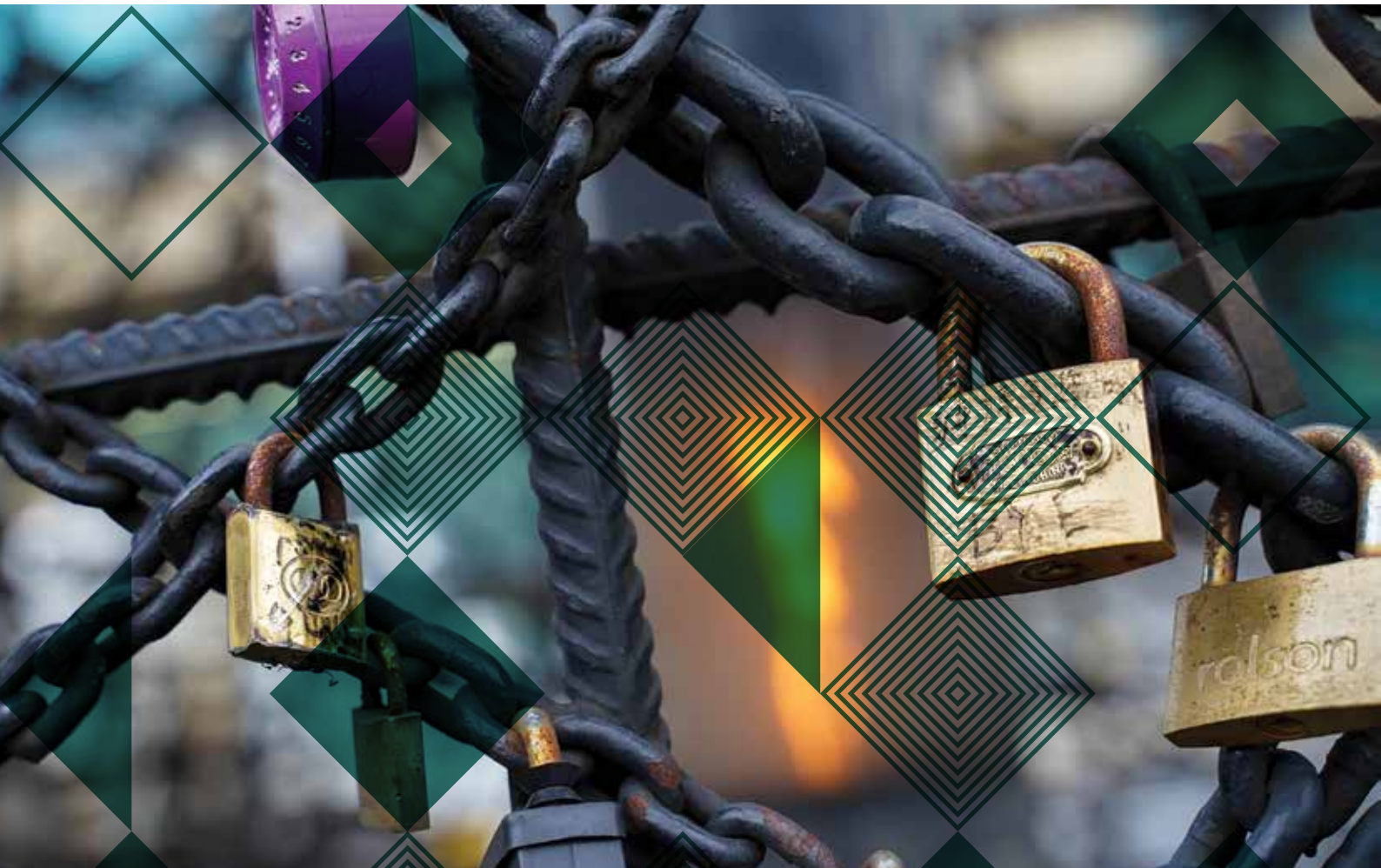
OSS Cooperation

The EU data protection legal framework has introduced a new era in cooperation between EU data protection supervisory authorities. The DPC has transitioned from a legislative environment in which it enjoyed exclusive competence to one that provides a harmonised approach to the application of data protection rights and obligations across the EU. As previously referenced, under the OSS model the DPC is the lead supervisory authority with oversight of the cross-border processing operations of personal data by many multinationals, including technology and social media companies.

In preparation for the GDPR, the DPC established a new OSS Operations team to coordinate all the EDPB cooperation and consistency procedures involving the DPC. This ensured that the DPC actively tracked and reported on its cross-border cases, handled the exchange of information with other supervisory authorities efficiently, and delivered its obligations on timelines and procedural steps. Between 25 May 2018 and 31 December 2018, the DPC team developed significant expertise in the EU IMI system, which is used for sharing information on cross-border cases between EDPB Supervisory Authorities.

EU Data Protection Supervisory Bodies

During 2018, the DPC continued to actively participate in the work programmes of the EU Supervisory Bodies for large-scale EU IT systems such as Europol, Eurodac, the Customs Information System (CIS), the IMI database and the Joint Supervisory Body of Eurojust. In addition, we continued to participate as observers of the coordinated supervision of the Schengen and Visa Information Systems (SIS II and VIS). With regard to SIS II, during the course of 2018, the DPC worked alongside An Garda Síochána and the Department of Justice & Equality in relation to Ireland's application to participate in certain non-border aspects of the Schengen acquis. This included a European Commission-led data protection evaluation, which took place in Ireland in November 2018. The work programme to progress Ireland's application will continue in 2019.



International

The DPC also engages extensively with international organisations and supervisory authorities outside of the EU to share information on practices in the context of enforcement and other regulatory activities.

Commissioner for Data Protection Helen Dixon and Deputy Commissioner Dale Sunderland travelled to New York in October to speak to stakeholders, including the New York State Bar Association's International Data Privacy and Protection Committee. The DPC took the opportunity to engage in bilateral meetings with several companies.

Members of the SMC of the DPC took part in many of the events at the International Conference of Data Protection and Privacy Commissioners (ICDPPC) in Brussels, which also took place in October. The ICDPPC is a global forum for data protection authorities to share knowledge and insights. The annual global conference — titled 'Debating Ethics: Dignity and Respect in Data Driven Life' — took place over six days.

The DPC's Head of Communications, Graham Doyle, attended the BIIDPA meeting in 2018 on behalf of the DPC. The DPC's participation in this annual conference led to bilateral sharing of best practices with other participants in areas such as operational improvement.

2018 GPEN Sweep

2018 saw the Global Privacy Enforcement Network (GPEN) conduct its 6th annual privacy sweep. The DPC, in conjunction with data protection authorities around the globe, participated in the sweep, the theme of which was privacy accountability. Accountability is a key element of GDPR. The concept of accountability requires organisations to take necessary steps to implement applicable data protection rules and requirements, and to be able to demonstrate how these have been incorporated into their own internal privacy programs. The aim of the sweep is to assess how well organisations have implemented accountability into their own internal privacy programs and policies and to establish a baseline of an organisation's compliance with data protection legislation.

In Ireland, the sweep was conducted by the DPC, which contacted 30 randomly selected organisations across a range of sectors (including pharmaceutical, multinational, government/local government, transport, charity, education and finance) and asked them to complete a suite of pre-set questions relating to privacy accountability.

After the introduction of the GDPR in May 2018, it was agreed by GPEN members that the 2018 sweep would be delayed until the final quarter of that year. Consequently, the final coordinated results will not be published until 2019. However, from an initial examination of the results of the Irish sweep, the DPC noted the following trends:

- 86% of organisations have a contact for their DPO listed on their website. We noted that all have privacy policies that are easily accessible from the homepage.
- Most organisations appear to have policies and procedures in place to respond to requests and complaints from individuals.
- 75% of organisations appear to have adequate data-breach policies in place.
- All organisations appear to provide some form of data protection training for staff. However, only 38% of those organisations provided evidence of training programmes for all staff, including new entrants and refresher training.
- In most cases, organisations appear to undertake some data protection monitoring/self-assessment, but not to a sufficiently high level. Three of the 29 respondents scored 'poor' in this section, while 13 reached 'satisfactory'.
- One third of organisations failed to provide evidence of documented processes to assess risks associated with new products and technology. However, most organisations appear to be aware of the need for this and many are in the process of documenting appropriate procedures.
- 30% of organisations failed to demonstrate that they had an adequate inventory of personal data while almost half failed to maintain a record of data flows.

The results of the sweep, when finalised, will assist the DPC in assessing what follow-up action is necessary.

13 Communications

During the period 25 May — 31 December 2018, the DPC continued, and expanded, its awareness-raising activities, now established as one of the DPC's tasks under Article 57 of the GDPR. During this period the DPC recruited staff skilled in communications and digital media production, and commenced an ambitious communications strategy comprising a number of streams.

Public information and guidance

The DPC continued to produce and disseminate industry-leading guidance documents for both the public and organisations to raise awareness of changes in the law, provide practical advice and guidance, as well as clarification and guidance on certain specific issues. Some of the topics on which the DPC produced information and guidance during the period 25 May — 31 December 2018 included:

- Guidance for Drivers on the use of "Dash Cams";
- Data Protection and Community Based CCTV Schemes;
- A practical guide to Data Controller to Data Processor Contracts;
- Canvassing, Data Protection & Electronic Marketing;
- Elected Representatives, the General Data Protection Regulation and the Data Protection Act 2018;
- Personal data transfers to and from the UK in the event of a 'no deal' Brexit; and
- Data Processing Operations that require a Data Protection Impact Assessment.

Direct engagement

The DPC maintained an active outreach schedule during the period 25 May — 31 December 2018, engaging with a broad base of Irish and international stakeholders. The Commissioner and her staff spoke, presented or otherwise contributed at events on over 110 occasions during this period, including conferences, seminars, and presentations to individual organisations from a broad range of sectors. Examples include:

National

- Data Summit 2018
- PDP Annual Data Protection Conference 2018
- Sunday Business Post, Post-GDPR Summit
- ISME Annual Conference 2018

International

- Fourth Bitkom Privacy Conference, Berlin
- Privacy Laws and Business 31st Annual International Conference, Cambridge
- 40th International Conference of Data Protection and Privacy Commissioners, Brussels
- International Association of Privacy Professionals (IAPP) Europe Data Protection Congress 2018, Brussels
- British, Irish and Islands Data Protection Authorities (BIIDPA) 2018 Annual Meeting, Isle of Mann

Media engagement

The profile of the DPC has never been higher, and continues to grow. This has been driven by factors such as the application of the GDPR, increased mainstream understanding of data protection issues, and the increasingly frequent data-related stories appearing in the national and international media.

The DPC is widely looked to for leadership on data protection issues, especially given the number of high profile multinational technology companies with European headquarters in Ireland. This has led to a significant increase in media interest in, and engagement with, the DPC. During the period from 25 May — 31 December 2018, the DPC engaged extensively with domestic and international media. Domestically, the Commissioner and other senior staff appeared on national television, were frequently interviewed across a variety of radio stations and contributed proactively and reactively to print and digital media. Internationally, the DPC appeared on Sky News, CNBC and CBS "60 minutes" programme speaking about issues from the application of the GDPR to the DPC's regulation of the multinational technology sector.

Web presence

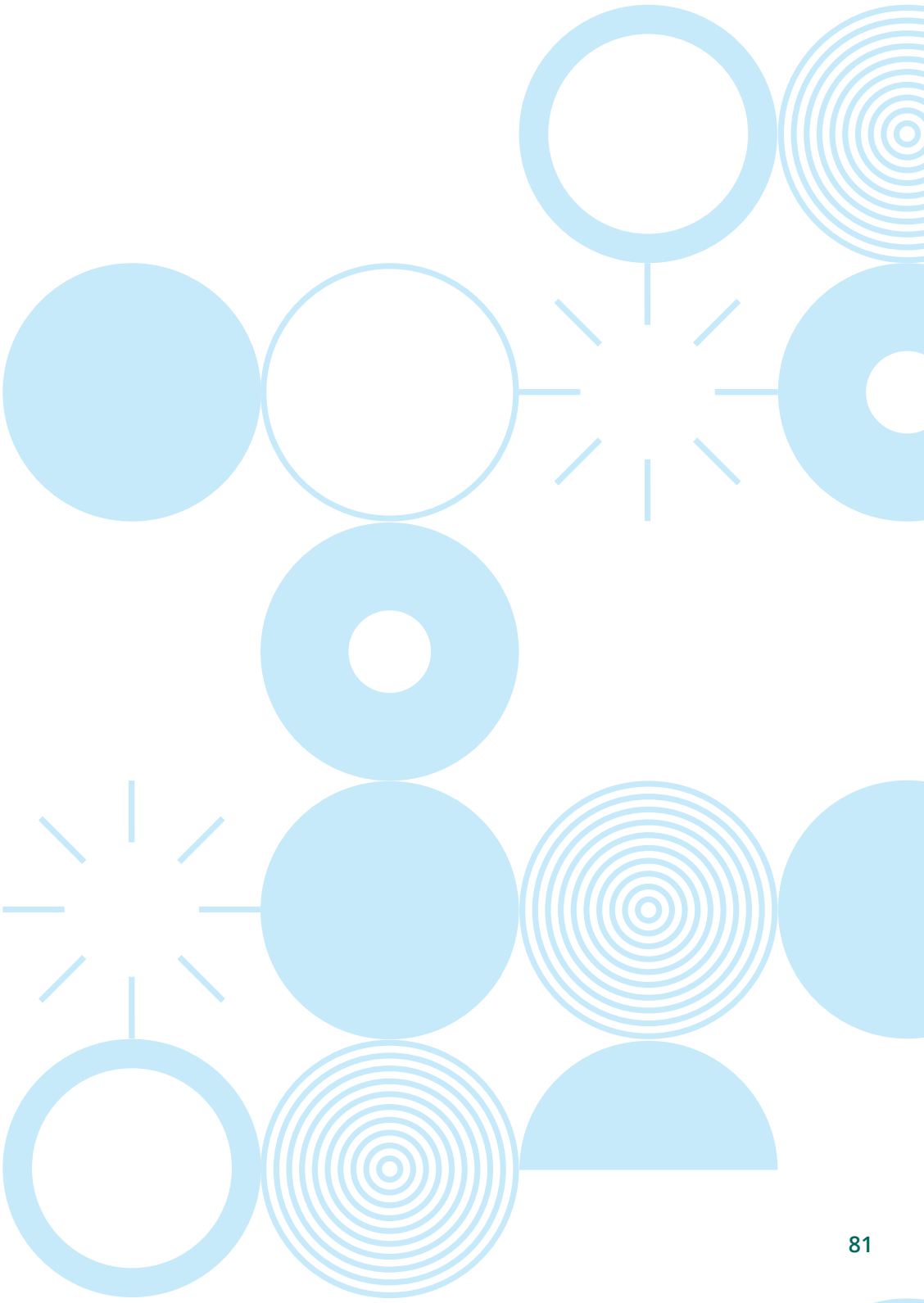
In the period immediately following 25 May 2018, the DPC website was updated with critical guidance for individuals and organisations necessary for engaging with the office for GDPR-related matters. The DPC also maintained its www.GDPRandYou.ie microsite, serving as a central hub for its GDPR-related resources.

In Q4 of 2018, there was a major redesign and relaunch of the main DPC website, www.dataprotection.ie. The new website offers extensive guidance and resources for the public as well as for data controllers and data processors that has either been updated or newly developed for the DPC's new statutory frameworks. Complaints, data breach notifications and general queries can now be submitted to the DPC through its online webforms.

Social Media presence

Social media continued to be an important forum for the DPC in support of its awareness-raising and communications activities. In the period from 25 May — 31 December 2018, the DPC expanded its social media activities across the Twitter and LinkedIn platforms, and at year end had a combined followership of approximately 10,000, and an organic monthly reach in the hundreds of thousands.

The DPC has enhanced 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 activities. With the roll-out of the DPC's communications strategy for 2019, the Communications Unit will further develop its social media content and will produce and disseminate podcasts and webinars through its social media channels, including its new Instagram account.



14 DPC's Consultations on "Children" and "Regulatory Strategy"

Public Consultation on the Processing of Children's Personal Data and the Rights of Children as Data Subjects Under the GDPR

Under the GDPR, all data protection supervisory authorities such as the DPC have a specific obligation to promote awareness and understanding of the risks, rules, safeguards and rights of data-processing activities involving children. Ahead of the GDPR entering into application on 25 May 2018, the DPC established a Children's Policy Unit, which sits within the Legal Division. This unit is headed by an Assistant Commissioner reporting to a Deputy Commissioner (Head of Legal), and from early 2018 exploratory work was underway in the DPC to look at how best to promote awareness and understanding of issues concerning the processing of children's personal data, the specific standards of protection for children under the GDPR and the rights of children as data subjects. Having engaged with a range of stakeholders in the areas of children's rights, promotion of children's interests and child protection, the DPC decided that in light of the significance attributed to children's issues under the GDPR this merited the development of a special consultation to collect the views on these issues of all stakeholders, most importantly children. Preparations for the consultation were ongoing throughout 2018, with a number of staff working full time on the project to develop and test materials for use in the consultation. The DPC was anxious to ensure that children, as the key stakeholders, had their say throughout. For this reason, and having engaged with the Ombudsman for Children's Office, the DPC decided that, separate to conducting an online written consultation for adult stakeholders, it would also directly consult with children by inviting schools and Youthreach centres to take part in a specially designed part of the consultation.

Intensive work on the development and refinement of materials for both streams of the consultation was ongoing throughout 2018. The first stream was launched on 19 December 2018, with a closing date of 1 March 2019 (Edit: date has been extended to 5 April 2019), on the DPC's website and social media platforms, with advertisements also running in national newspapers during the week of the launch and through the Government Public Consultations Portal on gov.ie. This stream aimed to engage adult stakeholders, including parents, educators, organisations that represent children's rights, child-protection organisations, representative bodies for parents and educators, and organisations that collect and process children's data. The online consultation document explained key concepts concerning the processing of children's personal data, the specific standards of data protection applicable to children, and the rights of children as data subjects, and posed a series of 16 questions, inviting submissions on any or all the issues raised.

The second stream launched on 28 January 2019. This stream, in which the DPC has been supported by the Ombudsman for Children's Office in the development and testing of the format and materials, seeks to involve children and young people (aged 8 and above) in the consultation process through classroom-based activities and discussions, facilitated by teachers using teaching materials that have been specially designed by the DPC for this purpose. All primary and post-primary schools and Youthreach centres nationwide have been invited to participate in this stream of the consultation, which has a closing date of 5 April 2019.

The DPC will use the responses from both streams of its consultation during 2019 to produce guidance materials for children and young people, and the organisations that process the personal data of children and young people. The DPC also intends to publish a statistical report, following the close of the consultation and its initial analysis of submissions; this will focus on themes such as participation levels and composition of participants in the consultation and headline trends according to stakeholder groups. Following the consultation, as a medium-term objective, the DPC will also work with industry, government and voluntary-sector stakeholders and their representative bodies to encourage the drawing-up of Codes of Conduct to promote best practices by organisations that process the personal data of children and young people, in accordance with the DPC's specific obligation under Section 32 of the Data Protection Act 2018.

DPC Regulatory Strategy

During 2018, the DPC invested significant resources and effort in clarifying its regulatory procedures to a very detailed level. However, we did not lose sight of the bigger picture; we also considered the wider context in which those regulatory procedures are executed and the need to frame our regulatory priorities and actions clearly. We have concluded that a comprehensive and wide-ranging analysis of the DPC's long-term regulatory strategy is vital. That internal consideration and reflection during late 2018 will turn outwards during 2019.

In late 2018, the DPC commenced a significant project to develop a new five-year DPC regulatory strategy. This will include extensive external consultation during 2019, which will be central to the analysis, deliberation and conclusions on our enduring strategy. This regulatory strategy will ultimately be our guide to how we fulfil our obligations, how we prioritise our statutory and non-statutory work, and how we strategically balance competing demands in the exercise of our regulatory powers to maximise the protection of personal data for all. Our ultimate strategy will continue to place citizens at the centre of how the DPC carries out its statutory functions. In addition, the strategy will set out the DPC's regulatory priorities and give insight and greater certainty to organisations and individuals on how the DPC intends to regulate.

15 Data Protection Officers

The GDPR created a new obligation under Article 37 whereby certain organisations are required to appoint a designated Data Protection Officer (DPO).

An organisation is required to appoint a DPO where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; or
- the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or
- the core activities of the controller or processor consist of processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

Furthermore, at a national level, Section 34 of the Data Protection Act 2018 provides for regulations to be made by the Minister for Justice and Equality, specifying further circumstances in which the designation of a DPO may be required.

Role of the DPO

The 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. The DPO should be able to perform their duties and tasks in an independent manner. A DPO may be a member of staff at the appropriate level with the necessary training, an external DPO, or one shared by a group of organisations. All options are provided for in the GDPR.

Organisations are required to publish the contact details of their DPO and provide these details to their lead supervisory authority. This ensures that individuals (internal and external to the organisation) and the DPA can easily and directly contact the DPO without having to contact another part of the organisation.

The Establishment of the Role of DPO Within the DPC

The role of the DPO is the cornerstone of the GDPR accountability-based compliance framework. As a data controller for the personal data it processes, the DPC recognises the importance of meeting, and being seen to meet, the very same standards that it expects from the organisations it regulates. Accordingly, and to ensure compliance with the GDPR well in advance of 25 May 2018, the DPC appointed its first DPO in January 2018.

As noted above, 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 barrister with significant prior experience in ensuring practical compliance with data protection obligations from an organisational perspective, the DPC's DPO has the required expert knowledge of both data protection law and practice. In addition, as a senior member of staff of the DPC (at Assistant Commissioner grade), the DPC's DPO reports directly to the highest level of management of the DPC (its SMC), as required by the GDPR. The DPC considers its DPO role to be of fundamental importance for meeting the obligations that apply to the DPC as a data controller and to ensure the workload of the DPO is kept under review so that the role is adequately resourced and supported.

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. The tasks of the DPO in the DPC are broader than the minimum tasks set out in Article 39 of the GDPR. For example, the DPC's DPO takes the lead on initiatives in day-to-day tasks such as monitoring the DPO email inbox, acting as an intermediary between relevant stakeholders (i.e. data subjects, business units within the DPC etc.) and responding to data protection queries from DPC staff members. The DPC's DPO is also proactive in identifying and implementing longer-term strategic initiatives such as developing internal procedures for handling data subject requests, delivering training to all staff on key issues and advising on the DPIA process.

The DPC's operational experience to date has been that its DPO acts as a 'critical friend' to the DPC. The DPC, acting as a data controller, listens to and takes on board the advice and analysis of its DPO. 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 — like any DPO role when performed in compliance with the GDPR — not only serves the cause of data protection but also addresses organisational-risk exposure from multiple perspectives.

DPO Notifications to the DPC

Establishment of a new DPO notification system by the DPC

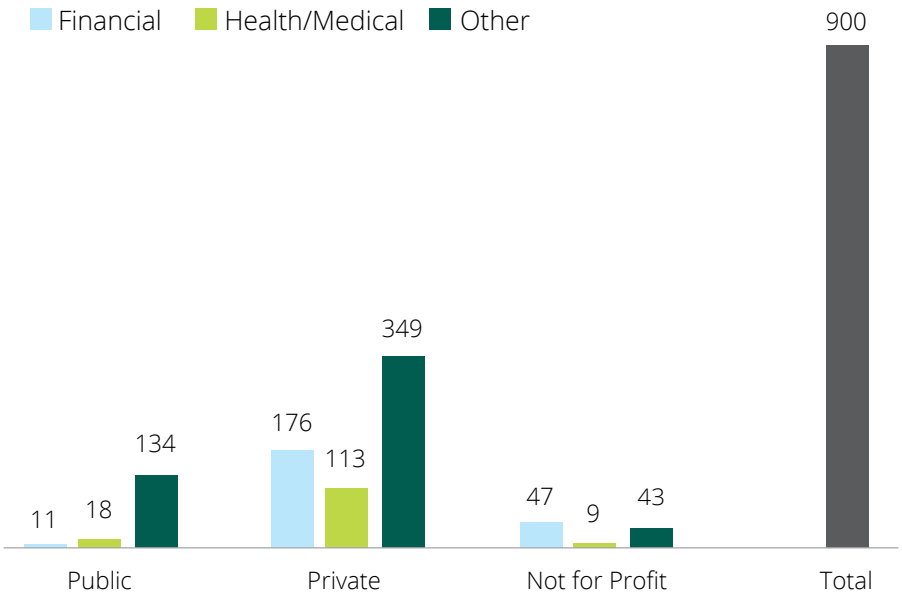
Prior to the application of the GDPR and the coming into force of the Data Protection Act 2018 on 25 May 2018, certain categories of data controllers and data processors were required to register with the former office of the Data Protection Commissioner. However, this legal requirement for registration has ceased and the DPC is no longer obligated to maintain a statutory register of data controllers and data processors.

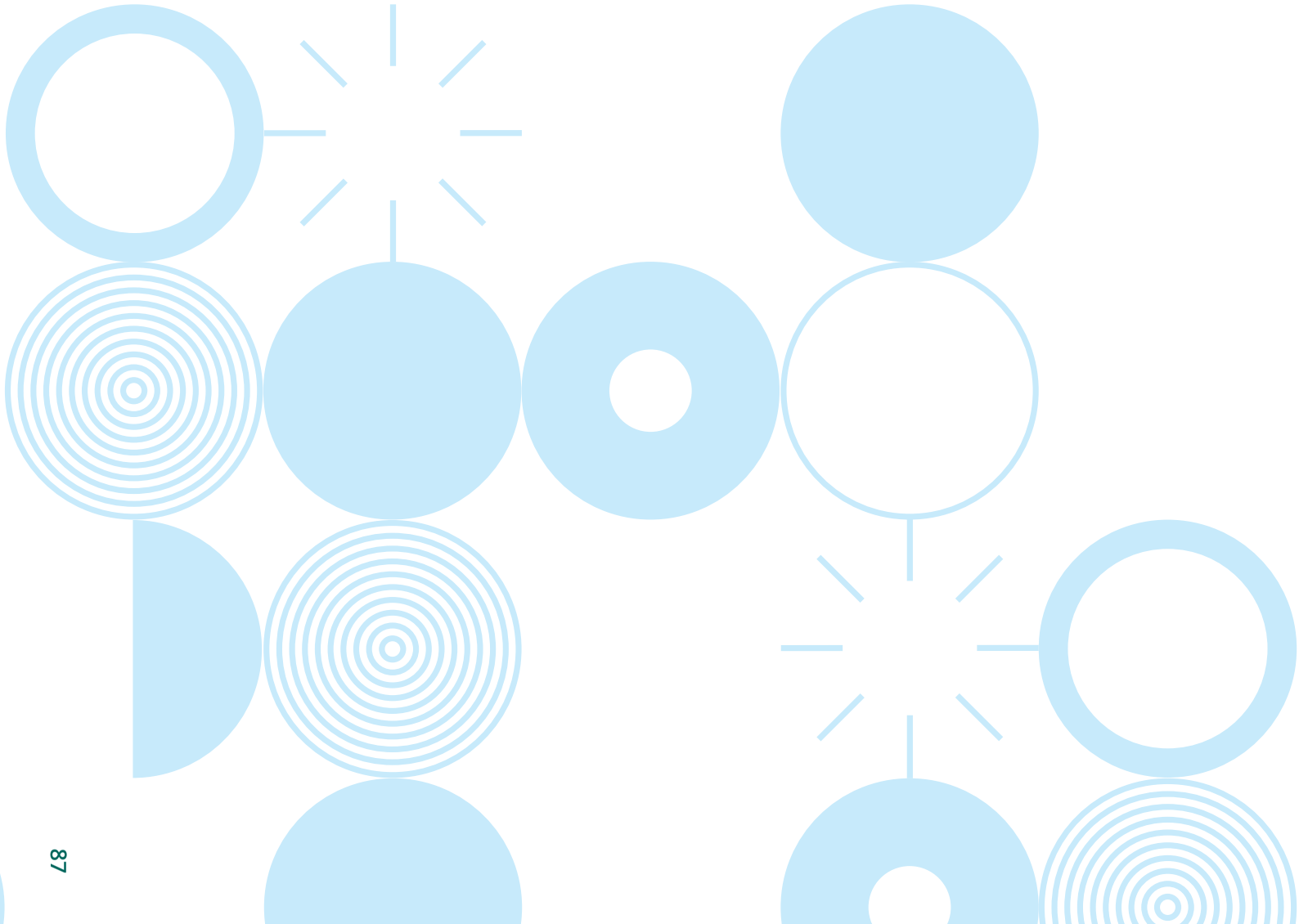
Under the GDPR however, data controllers and data processors required to designate a DPO are also required to report the contact details of the DPO to the relevant DPA.

Since 25 May, the DPC has established new procedures and information systems in order to receive notifications from relevant organisations about the designation of a DPO. The DPC has implemented a webform on its new website to this effect. There is no fee for this process. Between 25 May 2018 and 31 December 2018, the DPC received 900 DPO notifications. The chart below shows the industry sectors from which notifications were made.

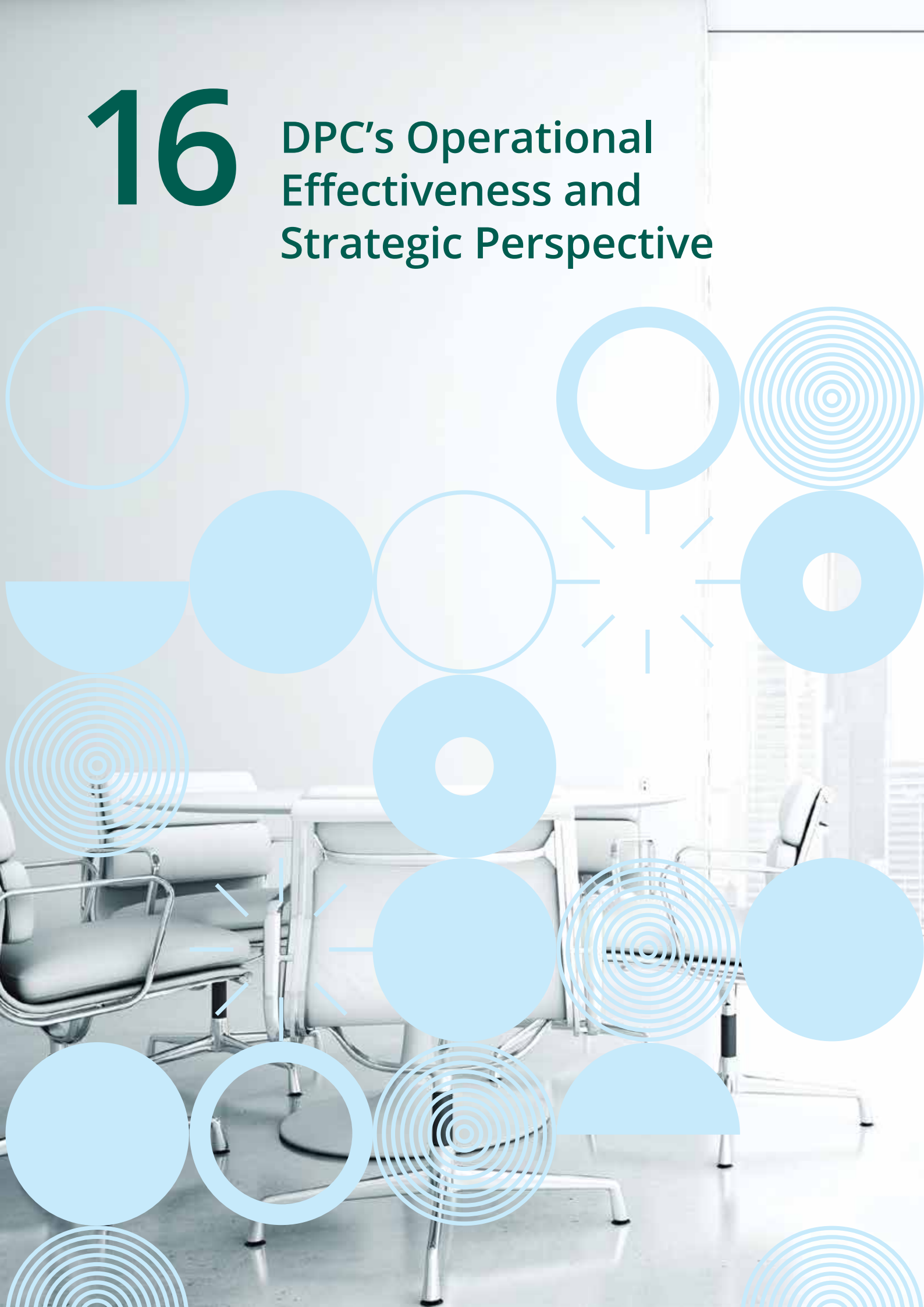
During 2019, the DPC plans to undertake a programme of work communicating with relevant organisations regarding their obligations under the GDPR to designate a DPO.

Statistics on DPO Notifications received by the DPC between 25 May and 31 December 2018





16 DPC's Operational Effectiveness and Strategic Perspective



Operational Effectiveness

Ahead of 25 May 2018, we successfully delivered our GDPR Readiness Programme, ensuring that the DPC was fully prepared to deliver its new and expanded functions on that date. Since 25 May 2018, we have continued to make progress on key elements of that programme covering procedures, processes, systems and technology. A new Operational Performance Unit was established at the DPC in the latter part of 2018 to drive this ongoing programme of change.

By dedicating resources to this unit, the DPC has underlined the importance of effective, efficient and consistent procedures, and the systems that underpin them, especially in the context of:

- our ongoing definition and implementation of standard procedures and process improvements in consideration of our new powers and duties under the Data Protection Act 2018;
- our collaboration with EDPB colleagues as we collectively address the practical implications of implementing the GDPR cooperation and consistency mechanisms;
- the DPC's continued growth in staff numbers and the need for procedural standards and system controls to ensure consistency and quality; and
- our increasing reliance on management information to inform our organisational decision-making as our casework volumes settle to new norms.
- Key achievements in support of our operational effectiveness between 25 May and 31 December 2018 were as follows:
- successful launch of the new DPC website, which allows individuals and organisations to access the DPC information they need much more easily and provides a full suite of webforms for contacting the DPC;
- operational adoption of the EU Internal Markets Information (IMI) system to manage information-sharing with other EDPB Supervisory Authorities, including proposals for system improvements, implementation of workarounds, and development of supplementary management information reports;
- completion of detailed analysis of the procedural implications of the Data Protection Act 2018, including the interplay with EDPB procedures and a comprehensive assessment of the impact on the data subjects and organisations with whom we interact; and
- finalising the detailed solution design and implementation plan for the new DPC case management and documents management system, due for implementation in 2019.

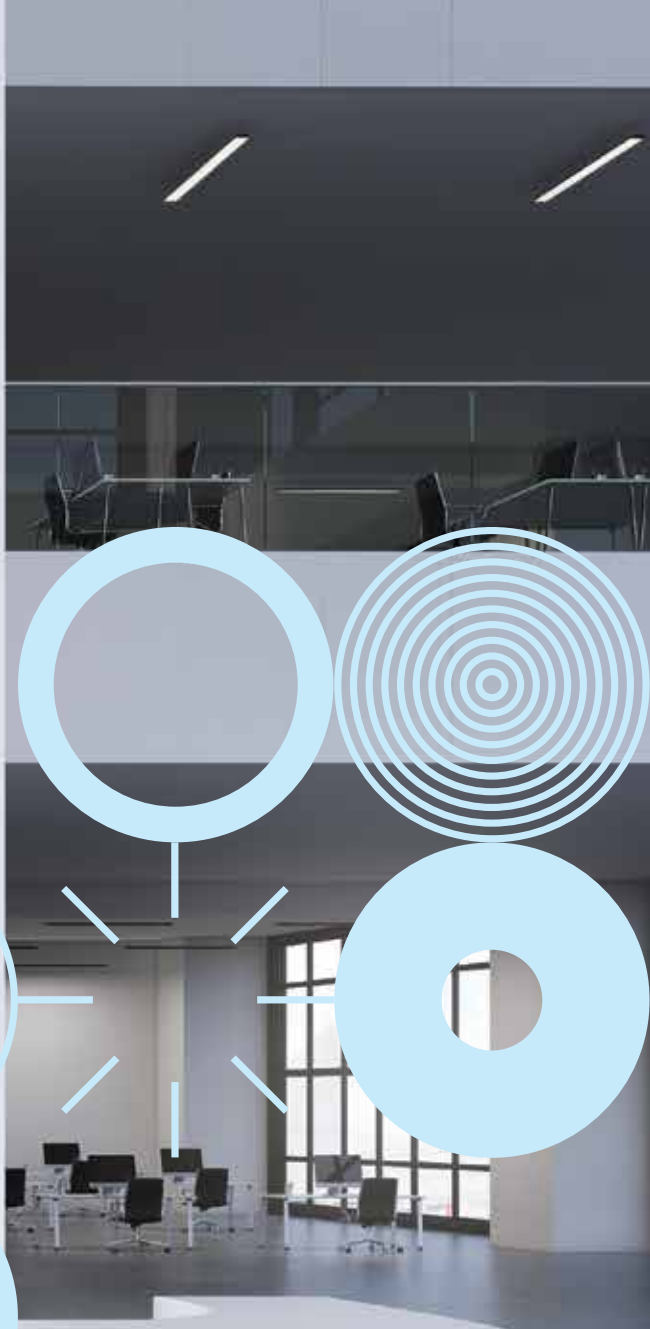
During 2019, priorities for this unit include finalisation and publication of our standard procedures, successful implementation of our new case management and documents management system, and implementation of new management information reports on all DPC activities.

Certification and Codes of Conduct

The DPC is also establishing a new unit to operationalise the important new mechanisms of Certification and Codes of Conduct that have been introduced by the GDPR. The accountability principle is emphasised throughout the GDPR, placing the onus on organisations to be compliant and be able to demonstrate that compliance. Certification and Codes of Conduct will enable organisations to demonstrate compliance voluntarily. This new DPC unit dedicated to these mechanisms will work to encourage their take-up and facilitate organisations as far as possible in implementing them successfully.

During 2018, the DPC acted as lead rapporteur and co-rapporteur respectively on the separate sets of EDPB Guidelines for Codes of Conduct and Certification, demonstrating the priority placed on these accountability mechanisms by the DPC. These guidelines are due to be published by the EDPB for stakeholder consultation in early 2019.

17
Corporate Affairs



Overview

The Corporate Affairs Unit plays a core role in supporting the DPC's strategic objectives and the performance of its statutory functions by ensuring that effective financial, HR, ICT and organisational services are in place. In addition, the unit is responsible for the development and implementation of measures to ensure the DPC's compliance with corporate governance requirements and other legislation.

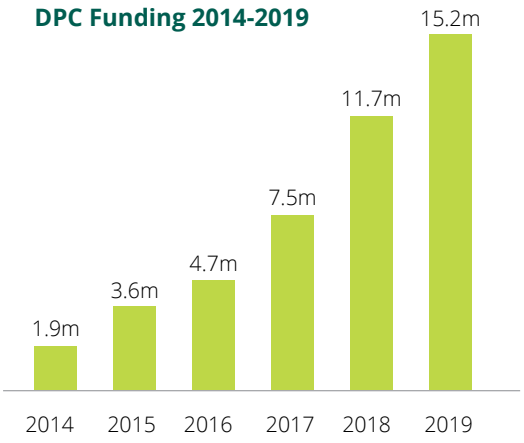
DPC Funding

The funding of the DPC by government has increased significantly in recent years from €1.7 million in 2013 to €11.7 million in 2018 (comprising a €7.3 million pay and €4.4 million non-pay allocation). The DPC very much welcomes the government's continuing commitment to enhancing the Irish data protection regulatory system and the DPC as a regulator. This continued commitment has allowed the DPC to grow its staff resources from 30 in 2013 to 110 at the end of 2018, thus enabling the DPC to perform its expanding role as one of the leading data protection authorities in the EU.

With the application of the GDPR and the new Data Protection Act 2018 on 25 May 2018, the DPC is now entirely funded by the Exchequer. There is no longer a legal requirement for specified categories of data controllers and data processors to register; consequently the DPC no longer collects revenue from this source.

The DPC's annual allocation is obtained via the Department of Justice and Equality Group of Votes under subhead A.7 entitled 'Programme A — Leadership In and Oversight of Justice and Equality Policy and Delivery'. For its payment and accounting processes, the DPC utilises shared services. Invoice payments are processed through the Department of Justice and Equality's Financial Shared Services Centre. The DPC's payroll and expense payments are processed by the national Payroll Shared Service Centre (PSSC), which is under the remit of the Department of Public Expenditure and Reform.

DPC Funding 2014-2019



Production of Financial Statements by the DPC

In accordance with Section 23 of the Data Protection Act 2018, the DPC is required to keep annual accounts of all funding received or expended, to submit those accounts to the Comptroller and Auditor General, and to arrange for the audited accounts to be laid before the Houses of the Oireachtas. The DPC is audited annually by the Comptroller and Auditor General.

The DPC observes the requirements set out in Public Financial Procedures and the Public Spending Code while also observing the expenditure and approval limits that apply to the Department of Justice and Equality.

For the year 2018, the DPC prepared two financial statements, the first covering the period of 1 January to 24 May 2018 in respect of the office of the Data Protection Commissioner, and the second covering the period of 25 May to 31 December 2018 in respect of the newly established DPC.

The Financial Statement of the DPC covering the period of 25 May to 31 December 2018 is in preparation for submission to the Comptroller and Auditor General for audit. Once the audit is concluded and the Financial Statement has been approved, it will be appended to this report.

DPC Staff Resources

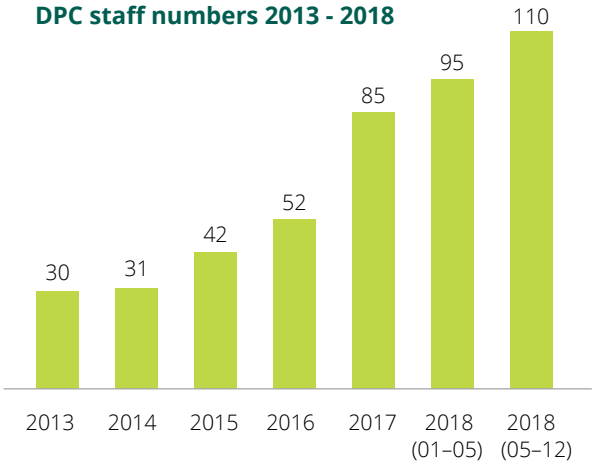
Throughout 2018, one of the most significant priorities for the DPC was to continue its programme of organisational change by expanding and developing its staff team. During the summer of 2018, the DPC, in close collaboration with the Public Appointments Service, undertook a major recruitment campaign involving five specialist competitions:

- Assistant Principal Officer — data protection team leads
- Assistant Principal Officer — senior legal advisors
- Higher Executive Officer — data protection executives
- Higher Executive Officer — legal advisors
- Higher Executive Officer — technologists

As a result of these campaigns, the DPC recruited significant numbers of new staff with a wide range of specialisms, including expertise in legal, technology, investigation and regulation areas. This major recruitment campaign has been critical in enabling the DPC to build a highly skilled workforce to deliver its expanded regulatory remit under the GDPR.

The DPC increased its staffing from 85 at the end of 2017 to 110 at the end of 2018. These staff are located across the DPC's Dublin and Portarlington locations.

DPC staff numbers 2013 - 2018



Furthermore, staff training and development continued to be a key priority for the DPC during 2018. Between 25 May and 31 December 2018, an intensive staff training programme was developed and delivered by the DPC's Legal Unit, with the purpose of enhancing the organisation's expertise and capability in the interpretation and application of data protection legislation, particularly the GDPR, LED and the new Data Protection Act 2018.

The DPC's strategic organisational expansion programme will continue to be a priority in 2019, with the DPC undertaking further staff recruitment campaigns, as well as devising and rolling out comprehensive training and development plans for DPC staff.

Project to Transition DPC to Become Its Own Accounting Officer

The Data Protection Act 2018, as well as establishing the Data Protection Commission as a new legal entity, also provides for the DPC to become independently and directly accountable for its statutory financial and human resource operations. This is currently planned to take place with effect from January 2020.

Between 25 May and 31 December 2018, the DPC commenced an organisational change programme, led by the Corporate Affairs Unit, to take over direct accountability for the DPC's financial, human resource management, information communications and technology needs, internal audit and governance functions. This has involved engagement with the Department of Justice and Equality on the transition and the scoping of those functions and activities that need to be transferred. This project will be a significant priority for the DPC during 2019.

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. 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 Department of Justice and Equality. As the DPC is independent in the performance of its functions under the provisions of the GDPR and 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 the period of this report is set out at Appendix III.

Risk Management

The Risk Management Policy of the DPC outlines its approach to risk management and the roles and responsibilities of the SMC, heads of units, 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 control and mitigate these risks.

The risk register is compiled by the Corporate Affairs Unit and 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 the period under review were as follows:

- Ensuring effective integration and consolidation of new 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.
- Building organisational capacity including developing the expertise of the DPC's staff as well as the continued recruitment of new staff with legal, specialist investigatory, and information technology skillsets in light of the new and enhanced functions of the organisation under the GDPR and national legislation.
- Making sure that the DPC has efficient and effective regulatory structures in place to carry out its mandate to protect the EU fundamental right to data protection and to uphold and enhance the integrity, professionalism and international reputation of the DPC.
- Ensuring that new business processes and appropriate internal controls are in place to directly manage functions such as financial, payroll, HR, ICT, and internal audit when the DPC transitions to becoming its own Accounting Officer.

Audit

The DPC's Internal Audit function is provided by the Department of Justice and Equality (DJE) Internal Audit under the oversight of the Audit Committee of Vote 24 (Justice).

The role of the DJE Internal Audit Unit is to provide independent assurance to the Accounting Officer on the effectiveness of the internal controls in place across the Vote. The DJE Internal Audit Unit assists the DPC by providing reasonable audit assurance that significant operating risks are identified, managed and controlled effectively.

The DJE Internal Audit Unit undertook an audit of the DPC's financial and governance controls in early 2018, with the report brought before the DPC's SMC and the DJE Audit Committee. The audit did not identify any significant issues. In addition, the DPC's daily interactions with citizens, businesses and other key stakeholders provides additional oversight of the DPC's work. Appeals of the DPC's statutory decisions can be made to the courts.

Other Statutory Obligations of the DPC

The Corporate Affairs Unit also manages and coordinates the implementation of other statutory and organisational obligations of the DPC including responding to freedom-of-information requests, data-subject requests, including subject-access requests, and customer-service requests and complaints to the organisation. In addition, the Corporate Affairs Unit manages and implements procedures regarding the DPC's compliance with its obligations under the Official Languages legislation.

Freedom of Information and Access to Information on the Environment

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. 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.

Between 25 May and 31 December 2018, the DPC received a total of 18 requests under the FOI Act. Of these, eight were deemed to be out of scope on the basis that they related to records held by the DPC other than the general administration of the office. A summary of the FOI requests received by the DPC between 25 May and 31 December 2018 is included in the table below. No cases were appealed to the Office of the Information Commissioner.

FOI Table

Request by type	Category total	Outcome
Administrative Issues	10	2 granted 1 refused 4 dealt with outside of FOI 3 withdrawn
Personal data (outside of scope)	1	
Matters outside the scope of the Acts	7	
Live cases	Nil	

As outlined in the Final Report of the Data Protection Commissioner (covering the period between 1 January and 24 May 2018), the DPC dealt with one request 'in year' during 2018 under the European Communities (Access to Information on the Environment) Regulations 2007, S.I. No. 133 of 2007. The decision issued was to refuse the information requested. An internal review of this decision was requested with the review upholding the original decision to refuse access to the information requested. On appeal, the DPC decided to release the information requested. This phase was completed during the time period covered by this report. There were two further requests between 25 May and 31 December 2018. One of these was a follow-on from the request made during the first part of the year and is now closed. The second request was refused. No internal review was requested with either.

Data-Subject Requests Including Subject-Access Requests

In accordance with the GDPR, the DPC is also a data controller in respect of personal data held by it and, as a result, the rights under Articles 12 to 22 and 34 of the GDPR may be exercised by data subjects. However, Article 23 of the GDPR permits member states to restrict the exercise of these rights by means of legislation, and these rights are restricted by Section 60(3)(c)(i) of the Data Protection Act 2018, which provides that these rights are restricted to the extent that personal data is kept by the DPC for the performance of its functions. The DPC interprets Section 60(3)(c)(i) in a manner that respects the essence of a data subject's rights and freedoms, and applies the restriction only so far as is necessary and appropriate. The Corporate Affairs Unit deals with such data-subject requests and works with other units across the DPC in responding to these requests.

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 our website.

Apendicies

Appendix I
Data Protection Case Law from the CJEU

Wirtschaftsakademie Schleswig-Holstein (Case C-210/16) (known as the 'Facebook Fan Pages' case)

Key issues: concept of controllership; national competence of a DPA.

Facts

Fan pages are user accounts that can be set up by individuals or businesses on Facebook, with non-negotiable conditions of use. Administrators of Facebook fan pages can obtain anonymous statistical data on visitors to the fan pages via a function called Facebook Insights. This data is collected by cookies that are placed by the fan page on a visitor's device or computer and which are active for two years. Wirtschaftsakademie is a private German company that offered educational services, including by means of a fan page hosted on Facebook. During the period in question, neither Wirtschaftsakademie nor Facebook notified visitors of the placement of cookies and the subsequent processing of personal data. By decision of 3 November 2011, one of the regional data protection authorities in Germany (the DPA) ordered Wirtschaftsakademie to deactivate its fan page due to the lack of notification in this respect. Wirtschaftsakademie challenged this decision on the basis that it was not responsible for the placement of the cookies nor the subsequent processing of personal data collected by way of the cookies. The ensuing legal proceedings ultimately resulted in the German Federal Administrative Court making a reference to the CJEU in relation to the 1995 Data Protection Directive (Directive 95/46/EC) on issues relating to who was responsible for the processing of the personal data and whether the German DPA could take action against Facebook Germany, which was responsible for advertising and marketing but not the processing of the personal data in question; that was under the responsibility of Facebook Ireland.

Judgment

The CJEU delivered its judgment on 5 June 2018. On the question of who was to be considered the data controller(s) of a Facebook fan page and therefore responsible for compliance with data protection law, the CJEU emphasised that this definition was to be interpreted broadly, in order to ensure 'effective and complete protection' of the persons whose personal data was being collected and processed. In practice, this means that more than one entity may be considered a joint controller. (Note that joint controllership is now specifically provided for under Article 26 of the GDPR, but was not provided for under the Data Protection Directive.)

The CJEU observed that Facebook Inc. and its subsidiary Facebook Ireland were 'controllers' responsible for processing the personal data of Facebook users and persons visiting the fan pages hosted on Facebook, as they primarily determined the purposes and means of processing that data. However, an administrator such as Wirtschaftsakademie must also be regarded as a controller, jointly responsible, within the EU, with Facebook Ireland for the processing of that data. The CJEU held that a fan page administrator, by creating such a page, gives Facebook the opportunity to place cookies on the device of a person visiting that page, whether or not they have a Facebook account. Such an administrator takes part by defining the parameters of the processing (depending in particular on its target audience and the objectives of managing or promoting its own activities) in the determination of the 'purposes and means of processing' the personal data of the visitors to its fan page. This influenced the processing of personal data for the purposes of producing statistics based on visits to the fan page, and the fan page administrator may 'even designate the categories of persons whose personal data is to be made use of by Facebook'.

While the fan page administrator received the statistical data in anonymised form, the CJEU held that this did not affect its designation as a controller as the Data Protection Directive did not require that, where there were joint controllers, each must have access to the data concerned. Equally the 'fact that an administrator of a fan page uses the platform provided by Facebook in order to benefit from the associated services cannot exempt it from

compliance with its obligations concerning the protection of personal data'.

However, the CJEU found that the existence of joint responsibility as joint controllers did not necessarily imply equal responsibility of all controllers and they might be involved at different stages of the processing and to different degrees so that the level of responsibility must be assessed by reference to all the circumstances of the case.

On the separate issue of the competence of German regional DPA, the CJEU found that it could exercise its national-law powers — for the purpose of ensuring compliance on German territory with the rules on the protection of personal data — against Facebook Germany because Facebook Germany was an establishment of the controller on Germany territory within the meaning of the Data Protection Directive. These powers could be used and intervention could be taken notwithstanding that Facebook Germany was responsible only for advertising and marketing activities and that Facebook Ireland was responsible for the data processing in question. Those powers of the German regional DPA were independent of the actions of another data protection authority on whose territory the controller (Facebook Ireland) was located and the German DPA did not have to first call on the other data protection authority to intervene before taking action itself.

Tietosuojavaltuutettu v Jehovan tod istajat (Case C 25/17) (known as the 'Jehovah's Witnesses Case')

Key issues: concept of controllership; application of the household exemption; meaning of 'relevant filing system'.

Facts

This case related to activities of members of the Jehovah's Witnesses Community whereby personal data is collected or processed in the course of door-to-door preaching by its members. The Finnish Data Protection Board (the Board) ordered the Jehovah's Witnesses Community to stop processing personal data unless they complied with Finland's laws implementing the Data Protection Directive (Directive 95/46/EC). The Board asserted that the collection of information by way of notes including names, addresses, religion and family status taken in the course of door-to-door preaching constituted processing but that this was done without the knowledge or consent of the persons concerned. The Board also found that both the religious community and its members were 'data controllers' for the purposes of data protection law. This was challenged, and the Finnish Supreme Administrative Court, asked by way of preliminary reference a number of questions around whether the activities in question and collection of personal data fell within the scope of the Data Protection Directive and whether the Jehovah's Witness Community itself was a controller jointly with its members.

Judgment

The CJEU's decision was delivered on 10 July 2018. The CJEU held firstly that the personal-data collecting activities in question fell within the scope of the Data Protection Directive as the exception for state security and similar areas did not apply to door-to-door preaching and could only apply to acts of the state. Secondly, the so-called 'household exemption' did not apply because it could not be said that the activities in question were purely personal or domestic in circumstances where the purpose is to make the data collected accessible to an unrestricted number of people or where that activity extends, even partially, to a public space and is accordingly directed outwards from the private setting of the person processing the data. While the processing activities fell within the activities covered by Article 10(1) of the EU Charter (freedom of thought, conscience and religion), the preaching extended beyond the private sphere in circumstances where, by its very nature, it is intended to spread the faith of the Jehovah's Witnesses Community among people who do not belong to that faith. Therefore it did not confer an exclusively personal or household character on that activity.

The CJEU also considered whether the personal data collected was contained within a relevant filing system as required in order for the Data Protection Directive to apply. The CJEU found that the Data Protection Directive broadly defined the notion of a 'filing system', which must be structured in order to allow easy access to personal data related to individuals. The Data Protection Directive did not lay down the practical means by which a filing system is be structured or the form in which it is to be presented. In the present case, the data collected in the course of door-to-door preaching were collected as a memory aid, according to geographical sector, in order to allow subsequent visits to people who had already been contacted, and to draw up lists of people who no longer wished to receive visits. Thus such data were structured according to criteria chosen to prepare for subsequent visits or keep lists of people who did not wish to be subsequently visited. The specific criteria for structuring the data was

irrelevant as long as it was possible for data relating to a specific person, who has already been contacted, to be retrieved. Accordingly, the personal data was contained within a relevant filling system within the meaning of the Data Protection Directive.

On the issue of controllership, the CJEU, referring to the Wirtschaftsakademie case (see above), stated that the concept of 'controller of the processing of personal data' may concern several actors. That did not mean, however, that every data controller had equal responsibility, or had to have access to the data to be a controller. However, a person who exerts influence over the processing of personal data, for his or her own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller. The collection and processing of personal data in the course of preaching by members was for the purposes of the Jehovah's Witnesses Community, which not only had knowledge of the processing carried out to spread its faith but actually organised, coordinated and encouraged the preaching activities of its members by allocating areas of activity and encouraging its members who engage in preaching to carry out data processing in the context of their preaching activity. As such, both the Jehovah's Witnesses Community and its members who engaged in preaching participated in determining the purposes and means of processing of personal data of the persons contacted and it was not necessary for the Jehovah's Witnesses Community itself to have access to the personal data or to have given its members written guidelines or instructions on the data processing in order for it to be a data controller.

Ministerio Fiscal (Case C-207/16)

Key issues: access to electronic communications data; justification for interference with fundamental rights; proportionality.

Facts

This case concerned the further application of the previous determination of the CJEU (in the Tele2 Sverige & Watson judgment, Case C-203/15 and C-698/15) that in the areas of prevention, investigation, detection and prosecution of criminal offences, only the objective of fighting serious crime can justify access by public authorities to personal data retained by electronic communications services, and that such access must be proportionate to the seriousness of the interference with the fundamental rights.

In this case, in the context of an investigation into the robbery of a wallet and mobile telephone, Spanish police made a judicial request for an order directing access to data held by electronic communication services providers, which would identify the users of telephone numbers activated with the stolen telephone. The request was rejected on the ground that the acts giving rise to the criminal investigation did not constitute a 'serious' offence — that is, an offence punishable under Spanish law by a term of imprisonment of more than five years. The Ministerio Fiscal (Spanish Public Prosecutor's Office) appealed against that decision before the Provincial Court.

The Spanish Provincial Court referred questions to the CJEU in relation to how to identify the threshold of seriousness of offences above which an interference with fundamental rights, such as national authorities' access to personal data retained by providers of electronic communications services, may be justified.

Judgment

The CJEU delivered its judgment on 2 October 2018, noting that national authorities' access, in connection with a criminal investigation, to personal data retained by providers of electronic communications services comes within the scope of the e-Privacy Directive (Directive 2002/58/EC on Privacy and Electronic Communications).

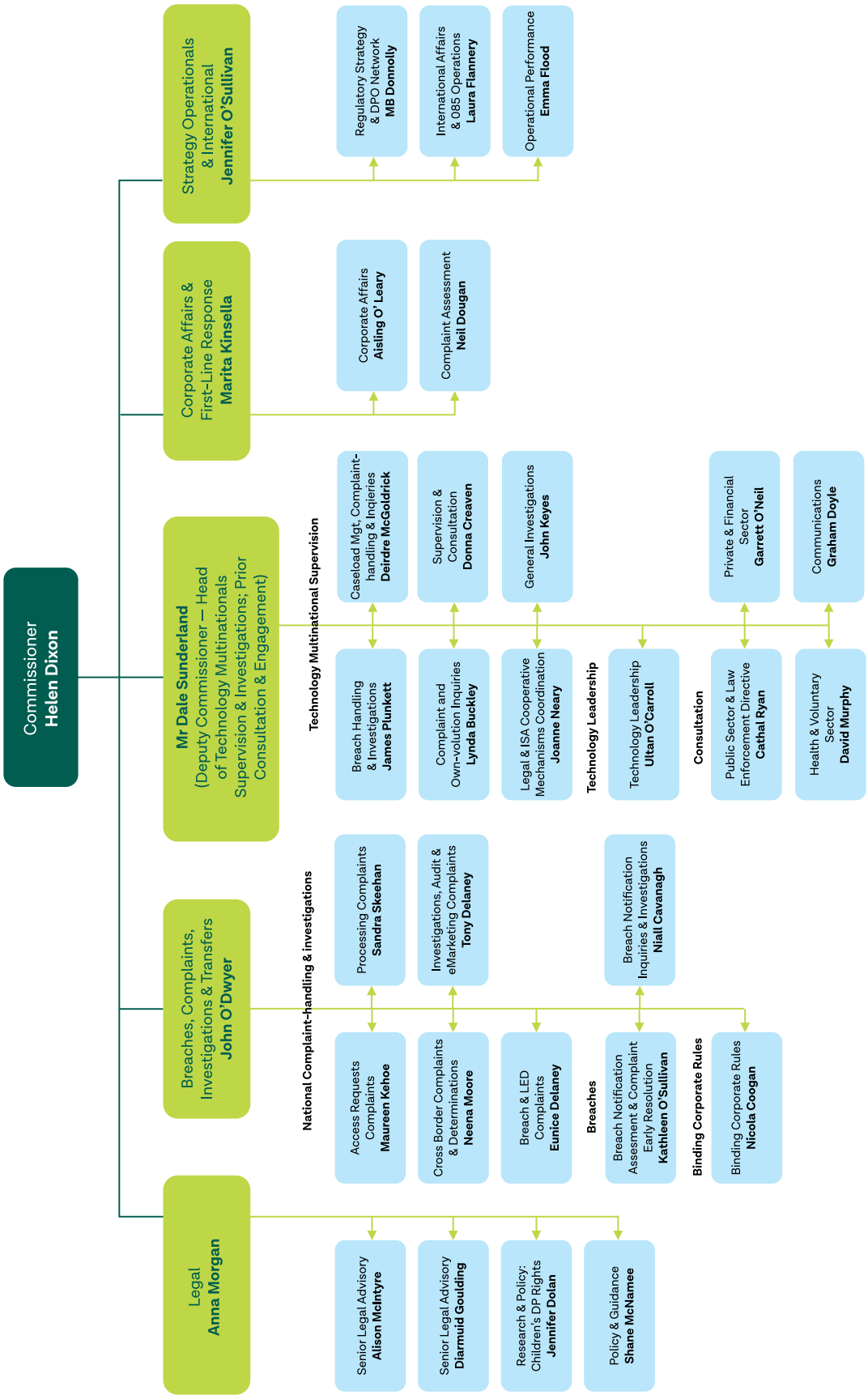
The CJEU reiterated that, in accordance with the principle of proportionality, serious interference with fundamental rights can be justified in areas of prevention, investigation, detection and prosecution of criminal offences only by the objective of fighting crime, which must also be defined as 'serious'. However, if the interference that such access to personal data entails is not serious, then the justification for access can be met by satisfying the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, rather than serious criminal offences.

In this case, the CJEU found that access to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as surnames, forenames and, if need be, addresses, did constitute an interference with such individuals' fundamental rights enshrined in the Charter of Fundamental Rights. However, this interference was not sufficiently serious to require that it could only be justified by the objective of fighting serious crime. This was because the data sought to be accessed did not allow precise conclusions to be drawn about the private lives of the individuals in question because it only enabled the SIM card or cards activated with

the stolen mobile telephone to be linked, during a specific period, with the identity of the owners of those SIM cards. Without those data being cross-referenced with the data pertaining to the communications with those SIM cards and the location data, the data sought did not make it possible to ascertain the date, time, duration and recipients of the communications made with the SIM card(s) in question, nor the locations where those communications took place or the frequency of those communications with specific people during a given period.

Accordingly, it was not necessary that access to the data in question had to be for the objective of fighting serious crime.

Appendix II
Organisation Chart



Appendix III
Statement on Internal Controls in Respect of the DPC Covering the Period of 25 May to 31 December 2018

Purpose of this Statement on Internal Controls

For the year 2018, the DPC prepared two Statements on Internal Control. The first was prepared in respect of the office of the Data Protection Commissioner to cover the period of 1 January to 24 May 2018.

This second relates to the newly established DPC, and covers the period of 25 May to 31 December 2018.

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 25 May to 31 December 2018 and up to the date of approval of the financial statements for that period.

Capacity to Handle Risk

The DPC reports on all audit matters to the Audit Committee in the DJE. The Audit Committee in the DJE met on four occasions between 25 May and 31 December 2018. The SMC of the DPC acts as the risk committee for the organisation. The Commissioner and senior managers from the DPC met with the DJE in 2018 and discussed audit and risk issues relating to the organisation.

The Internal Audit Unit of the DJE 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 2018.

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 2018.
- 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

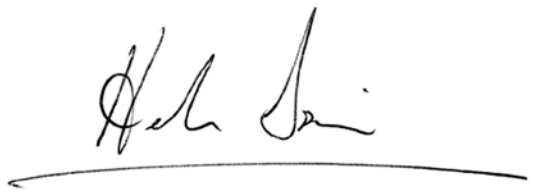
I confirm that the DPC has procedures in place to ensure compliance with current procurement rules and guidelines, and that between 25 May and 31 December 2018 the DPC complied with those procedures.

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 of the DJE carried out an audit at the DPC during 2018 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 25 May and 31 December 2018.



Helen Dixon
Commissioner for Data Protection

Appendix IV
Energy Report: 25 May to 31 December 2018

Overview of Energy Usage

DUBLIN

21 Fitzwilliam Square

The head office of the DPC in Dublin is based at 21 Fitzwilliam Square, Dublin 2. Between 25 May and 31 December 2018, the source of the main usage of energy in the office was electricity for heating, lighting and other uses.

As 21 Fitzwilliam Square is a protected building, it is exempt from the energy-rating system.

Satellite office

To accommodate an increase in staff, the DPC previously entered into a short-term agreement for the provision of additional office space in another building. During 2018, the DPC relocated this satellite office to accommodate the increase in staff numbers. This action was taken as an interim measure prior to the finalisation of a larger Dublin premises to accommodate the DPC's Dublin-based staff and operations. The DPC's energy usage information for these buildings is not currently available.

PORTARLINGTON

The Portarlington office of the DPC has an area of 444 square metres and is located on the upper floor of a two-storey building built in 2006. The main use of energy in the office was for gas and electricity for heating, lighting and other uses.

The energy rating for the building in Portarlington was C1.

Actions Undertaken

The DPC has participated/is participating in the SEAI online system in 2018 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 2017 (last validated SEAI figures available) is as follows:

Dublin office:

Usage	
Non-electrical	0
Electrical	77940 kWh

Portarlington office

Usage	
Non-electrical	45,203 KwH
Electrical	32100 KwH

The DPC has continued its efforts to minimise energy usage by ensuring that all electrical equipment and lighting are switched off at the close of business each day. We are currently replacing florescent-light units with more energy-efficient LED units on a phased basis. Other equipment in need of replacement in any DPC accommodation is replaced with a more energy-efficient model where appropriate.

Appendix V
Financial Statement for the Period of 25 May to 31 December 2018

For the year 2018, the DPC prepared two financial statements, the first covering the period from 1 January to 24 May 2018 in respect of the office of the Data Protection Commissioner, and the second covering the period of 25 May to 31 December 2018 in respect of the newly established Data Protection Commission.

The Account of Income and Expenditure of the office of the Data Protection Commissioner for the period from 1 January to 24 May 2018 has been prepared and submitted to the Comptroller and Auditor General. Following completion of the audit in respect of that period by the Comptroller and Auditor General, the Financial Statement will be appended to the Final Report of the Data Protection Commissioner and published on the DPC's website.

The Account of Income and Expenditure of the Data Protection Commission for the period of 25 May to 31 December 2018 is in preparation by the DPC and will be appended to this report following completion of an audit in respect of that period by the Comptroller and Auditor General.

Data Protection Commission,
21 Fitzwilliam Square,
Dublin 2.

www. dataprotection.ie
Email: info@dataprotection.ie
Tel: 0761 104 800
LoCall: 1890 25 22 31

An Coimisiún um Chosaint Sonraí
Data Protection Commission