Final Report

1 January - 24 May 2018

Presented to each of the Houses of the Oireachtas, pursuant to Section 66(4) of the Data Protection Act 2018.

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

The Data Protection Commissioner (DPC) is the national independent authority with responsibility for upholding the EU fundamental right of the individual to have their personal data protected.

Table of contents

APPENDICES

Foreword

Ms. Helen Dixon
Data Protection Commissioner

After 30 years that spanned the advent of the Fourth Industrial Revolution, the invention of the ubiquitous personal smart phone and the sequencing of the full human genome, the Irish Data Protection Commissioner is no longer. I am proud to have served as the final of five consecutive commissioners at the office of the Data Protection Commissioner who between them spanned the years 1988 to 2018.

The significant achievements of the office of the Data Protection Commissioner have been many over the years and I'm pleased to include in this final Report of the Data Protection Commissioner the reflections of Bob Clark (Emeritus Professor University College Dublin) on "30 years of Data Protection Rights in Ireland" (Appendix VIII) .

This final Report covers the period of 1 January 2018 to 24 May 2018 at which point the office of the Data Protection Commissioner ceased and the new Data Protection Commission (DPC) was created under the Data Protection Act 2018, which also gave effect to the General Data Protection Regulation (GDPR) in Ireland. The first five months of 2018 were a truly extraordinary time for the DPC. Business as usual had to continue with 1,046 complaints resolved, 1,198 breach notifications handled and a range of audits and inspections concluded. Our telephone and email query services were particularly busy, with over 9,900 emails and 10,200 telephone calls received during the period — an increase of around 30% on the preceding six months. In April 2018, arising from proceedings initiated by the DPC in May 2016, the Irish High Court issued its reference case for a preliminary ruling to the Court of Justice of the European Union, seeking its judgement in relation to the validity of Standard Contractual Clauses (SCCs) to legitimise transfers of EU personal data to the US. In a range of other Circuit Court and High Court litigation, the DPC continued to contribute to the growing body of case law interpreting data protection principles and provisions and these are set out in the Legal section of this Report of this report.

DPC contribution to prepare Ireland for the General Data Protection Regulation (GDPR)

The DPC invested significant resources in preparation for the application of the GDPR from 25th May. This work included: preparing the DPC for its new supervisory role; preparing all stakeholders for their new obligations and the public for exercise of their rights; and contributing to preparations by EU data protection authorities for a harmonised interpretation of the new law from May 2018. The GDPR is, of course, a game-changer — for organisations, for individuals and for data protection authorities. Organisational preparation intensified as we readied the ship for considerable change alongside a continuation of existing processes given the lack of retrospectivity of the GDPR and the Data Protection Act 2018. Recruitment continued at the pace of the previous three years with a range of new specialists added, bringing the team to around 110. In-house training programmes were rolled out to ensure all staff developed expertise in the changing legal framework. Particular challenges in this regard arose from the later-than-anticipated enactment of the Data Protection Act 2018, where late-stage amendments of particular significance to the DPC concerning the complaint-handling function were still in play. Mapping the changes in our hundreds of processes and mapping new processes in advance meant we could hit the ground running on 25 May — albeit our new website, web-forms and case management system are still being finalised. Coordination efforts in relation to the new Internal Market Information system (IMI) platform now used by EU data protection authorities to share information between each other and lodge cross-border processing cases ("One-Stop-Shop" cases) have been complex, but the DPC has been fortunate in recruiting an experienced business analyst to oversee this critical work.

Supporting organisations in preparing for the GDPR

Engaging with all types of organisations grappling with the GDPR was a particular focus of the first five months of the year. A high number of consultations were held and the genuine efforts of many organisations to understand what the GDPR requires and to strive to deliver on those standards was extremely encouraging. On January 23rd, the DPC partnered with the Centre for Information Policy Leadership (CIPL) to host a unique day-long event in Dublin Castle for SMEs and public-sector bodies. The event was not a GDPR conference but rather a GDPR "live demonstration" event. Global companies like HP and MasterCard with multi-million-euro data protection and privacy programmes, demonstrated in very pragmatic ways, how they are implementing the accountability provisions of the GDPR — what does a documented set of data processing operations under Article 30 actually look like and how do you go about the task? Based on the feedback received, the event was a huge success and a real contributor to higher levels of practical knowledge in Ireland regarding what the GDPR requires.

In early March, accompanied by a Deputy Commissioner, I travelled to San Francisco and the Bay Area to meet with a whole range of companies that are required to comply with the GDPR. The trip was useful in gaining an understanding of those aspects of the new law that were creating confusion for organisations, such as the role of the Article 27 representative in the EU where an organisation has no EU establishment. What was clear from the meetings was that consideration of many of the newer features of the GDPR were lower down the list of immediate priorities of organisations. What was equally clear is that the world's most innovative companies have yet to come up with equally innovative solutions to deliver real personal data transparency and useful information to users, while delivering a positive user experience.

Awareness-raising with members of the public

In relation to broader awareness-raising activities in the first five months of the year, the DPC sought to engage members of the public as well as organisations, running cinema and radio ads in particular to highlight the new rights and obligations under the GDPR. Over 80% of Irish adults were reached through these campaigns and a survey commissioned on behalf of the DPC showed almost a 90% awareness amongst SMEs of the new law. Without awareness, there cannot be compliance and the DPC is proud to have been part of the broader stakeholder community that contributed to driving very high levels of awareness of the GDPR in Ireland.

Awareness-raising around the GDPR and data-protection laws received an unfortunate boon in March with the Observer/Guardian newspaper disclosures of allegations of misuse of Facebook data by a UK analytics company, Cambridge Analytica. While many people now understand the basic revenue model of free internet services that relies on collecting as much individual data as possible from users for personalised targeted advertisements, it came as a shock to many to discover the data could potentially end up in the hands of third parties seeking to influence election outcomes. The need to find an effective means to be truly transparent with users in relation to uses of their data on and off online platforms is critical at this stage. As EU regulators we need to figure out the ethical standards for transparency and what privacy by design and default should look like, and impose them. Because it's clear that mere technical compliance with the GDPR is not an overly challenging hurdle in relation to the transparency requirements set down in Articles 12 -14 of the GDPR. However, mere compliance by organisations does not necessarily add up to effective understanding on the part of individuals of the deal to which they are signing up.

As one door closes, another opens……

Which brings me on to the future as we look forward to the new era of the DPC with increased powers and a new legal framework. The changes at the new Data Protection Commission are infinitely more than a new logo. As a regulatory body, we have a firm grasp of the challenges that face all of us in maintaining and exercising control over our personal data. We are motivated to handle complaints from individuals and to deliver results that are fair and grounded in the new law. Equally, we will take all available opportunities to pursue broader data protection issues of concern to the public at large. The new One-Stop-Shop mechanism under the GDPR places the DPC in a central position in monitoring and enforcing the application of the GDPR at the world's largest internet companies. Already, we are in receipt of multiple complaints that require us to address fundamental issues in relation to the legal bases for collection of data by platforms and the adequacy of information provided to users. These also require us to take account of the views of other EU data protection authorities as we finalise our findings.

We will launch a process of consultation around a GDPR-term regulatory strategy for the DPC before the end of the first quarter of 2019 that will provide sustainable and transparent underpinning for what are inevitable resource deployment options and choices and which will provide an element of certainty to organisations and the public in relation to the DPC's role and how that role will be implemented. In addition, the DPC will run a focussed consultation commencing later this year on the exercise of rights by children under the GDPR and around issues relating to the specific data protection safeguards that should apply to children at different developmental stages. The DPC will be supported by the Ombudsman for Children's Office in this work and the end result of the consultation will be detailed guidance for delivering specific protections for children. In turn, this will provide underpinning for industry and relevant stakeholders to develop and propose a Code of Conduct in line with Section 32 of the Data Protection Act 2018 and Article 40 of the GDPR.

Farewell to the office of the Data Protection Commissioner. The new Data Protection Commission looks forward to a future of enhanced data protection rights under the GDPR.

Helen Dixon
Data Protection Commissioner

Roles and Responsibilities of the Data Protection Commissioner

Purpose of this Report

A new data protection legal framework applies across the EU since the application of the GDPR on 25 May 2018. In addition, on that date, the Data Protection Act 2018 established a new Data Protection Commission (DPC) and transferred all of the functions of the Data Protection Commissioner to the new Commission.

In accordance with Section 66 of the Data Protection Act 2018, this Report has been prepared as a final Report in respect of the office of Data Protection Commissioner and it covers the period from 1 January to 24 May 2018.

Roles and Responsibilities of the office of the Data Protection Commissioner

The office of the Data Protection Commissioner was established under the Data Protection Act 1988 with responsibility for upholding the fundamental right of the individual to have their personal data protected. The functions, duties, and statutory powers of the Office were set out in the Data Protection Acts 1988 and 2003, which transposed the Council of Europe Convention 108 and the 1995 Data Protection Directive.

The Data Protection Commissioner and the staff of her office were mandated under the Data Protection Acts 1988 and 2003 to supervise compliance with data protection legislation and identify risks to the protection of personal data. This purpose has been achieved in a number of ways including through:

- the investigation of complaints from individuals,
- proactive engagement and consultation with a wide range of public and private sector organisations involved in the processing of personal data,
- activities to improve compliance with data protection legislation and the publication of high-quality guidance,
- the conduct of on-site inspections and audits of organisations, and
- the taking of enforcement actions were necessary.

In addition, the office of the Data Protection Commissioner played an active and engaged role at EU level. The Office worked closely with other European Data Protection Authorities (DPAs) and actively engaged in the work of the Article 29 Working Party. Throughout 2017 and during the period covered by this Report, in preparation for the advent of GDPR the office worked closely with its EU colleagues to drive harmonisation of data protection rules and procedures and plan for the application of GDPR on May 25 2018.

Since 25 May 2018, the office of the Data Protection Commissioner has transitioned into the new Data Protection Commission (DPC) with an expanded regulatory remit, as provided for under the General Data Protection Regulation (GDPR), Directive (2016/680) concerning personal data processing in a law enforcement context (Law Enforcement Directive) and the Data Protection Act 2018. In accordance with this new legislation, the DPC is no longer a data protection authority with a national focus, but has become a supervisory authority with an EU-wide remit responsible for protecting the data privacy rights of users across the EU.

DPC Senior Management Committee

In recognition of the significantly increased funding and the rapidly growing size of the organisation, the DPC established the Senior Management Committee (SMC) in 2016 comprising the Commissioner and Deputy Commissioners.

The Commissioner and the 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 Senior Management Committee comprises:

- **Ms. Helen Dixon** (Data Protection Commissioner);
- **Ms. Anna Morgan** (Deputy Commissioner — Head of Legal);
- **Mr. Dale Sunderland** (Deputy Commissioner — Head of Policy and Engagement and Multinationals and Technology);
- **Ms. Jennifer O'Sullivan** (Deputy Commissioner — Head of Strategy, Operations and International);
- **Mr. John O'Dwyer** (Deputy Commissioner — Head of Complaints and Investigations); and
- **Ms. Marita Kinsella** (Deputy Commissioner — Head of Corporate Affairs and First-Line Response).

Funding and Administration

The DPC is dependent on sufficient resources being provided by Government to fulfil its mandate as the independent supervisory body in Ireland for the protection of fundamental data protection rights. In recognition of the priority that the Irish Government places on upholding data protection rights and 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 an allocation of €11.6 million in 2018 (comprising €7.3 million pay allocation and €4.3 million non-pay allocation).

The DPC acknowledges the significant increase in funding in recent years and welcomes the Government's continuing commitment to resourcing needs the office 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. The DPC's 2018 allocation has not been divided as between the office of the Data Protection Commissioner (up to 24 May 2018) and the new Data Protection Commission (post 25 May 2018). The final Financial Statement for the office of the Data Protection Commissioner in respect of the period from 1 January to 24 May 2018 will be appended to this Report following the conduct of an audit by the Comptroller and Auditor General.

As per Part 4 of the 2018 Act, the DPC's 2018 allocation transferred to the new Data Protection Commission on 25 May 2018.

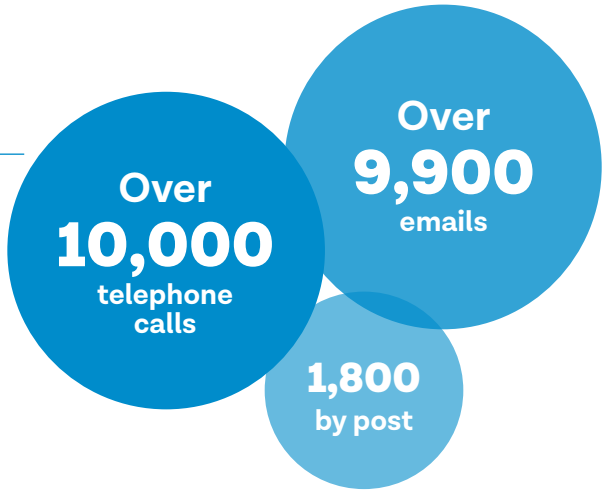
The office of the Data Protection Commissioner's main goals for 2018

In accordance with the DPC's Statement of Strategy 2017–2018, the main goals for the period covered by this Report are as follows:

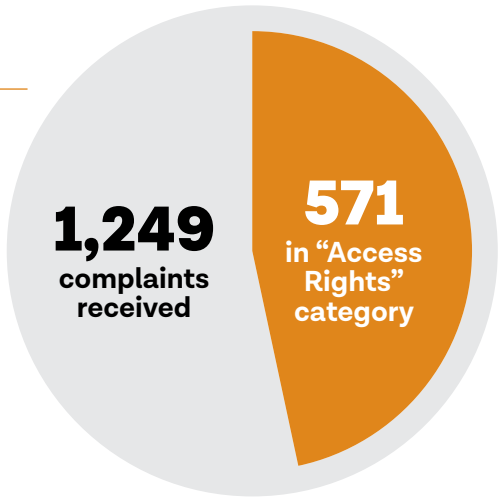
1. Further develop the capabilities and capabilities of the DPC to reflect our enhanced role under the new GDPR, Law Enforcement Directive and ePrivacy Regulation regime by:
    - » Proactively engaging with government to ensure we have the required regulatory powers, as well as financial and other resources, 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 our processes, systems (including our ICT capabilities) and structures, to ensure our continued effectiveness under the new data protection regime.
2. Collaborating 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 through 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. Ensuring 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 may 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 better improved compliance with data protection obligations through investigations and audits targeting high-risk and large-scale processing of personal data.

Review of 1 January – 24 May 2018 in Brief

- Our Information and Assessment Unit received almost **22,000** contacts comprising over **9,900** emails, **10,200** telephone calls, and approximately **1,800** items of correspondence via post. The month of May saw a significant increase in demand, with nearly **6,000** contacts made with the Unit in the month and an average of **270** contacts per working day.



- Total Complaints received was **1,249**, with the largest single category being "Access Rights" which made up 571 complaints or 45% of the total.



- **1,046** complaints were concluded from 1 January – 25 May.
- While the majority of complaints continued to be amicably resolved, we issued a total of **12** formal decisions.

- **1,198** valid data security breaches were recorded.

- **The Special Investigations Unit (SIU)** completed its investigation which examined the processing of patient sensitive personal data in areas of hospitals in Ireland to which patients and the public have access. The SIU published a report entitled "Data Protection Investigation in the Hospitals Sector" in May 2018 and it was disseminated to every hospital in the State.
- The SIU completed its investigation examining the governance by Tusla (the Child and Family Agency) of the handling of personal data concerning child protection cases in December 2017. The Unit presented its findings (59 in total under twelve topic headings) to TUSLA in January 2018.
- The SIU continued its work in the Private Investigator sector and inspections were carried out by members of the SIU at the premises of two private investigators. Work also continued in relation to the special investigation into the Public Services Card of the Department of Employment and Social Protection.
- **41** new complaints were investigated under S.I. 336 of 2011 in respect of various forms of electronic direct marketing.
- Direct marketing complaint investigations were completed during this period. A number of these investigations concluded with successful District Court prosecutions by the DPC. In this regard, prosecutions were concluded during this period against three companies in respect of a total of 46 offences under the E-Privacy Regulations. These prosecutions resulted in convictions on four samples charges and the application of the Probation of Offenders Act in relation to three charges.
- The number of general consultation queries received was **503**, mirroring the numbers received in 2017.
- Consultations with private and public sector organisations continued, to assist organisations in their preparations for the GDPR.
- **23 audits/inspections** were carried out. The aim of all audits/inspections is to check for compliance with the Data Protection Acts and to assist the data controller or data processor in achieving best practice in terms of its data processing operations.
- Regulatory engagement with multinational companies continued in preparation for the introduction of the GDPR.

- During the period 1 January to 24 May 2018 there were significant 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. Further hearings in the High Court on the issues of both the precise questions to be referred to the CJEU, and "errors" in the High Court judgment of 3 October 2017 which were alleged by Facebook and the US Government, took place in January. In April, the Court issued an amended version of its original judgment in which alterations were made to certain paragraphs of the judgment in response to the submissions on the allegations of "errors". The Court also decided on the specific questions to be referred to the CJEU in its request for a preliminary ruling.
- In May, the High Court refused an application by Facebook for a stay on the High Court judgment pending appeal, with the Court holding that the least injustice would be caused by doing so and by immediately delivering the reference to the CJEU. Facebook subsequently appealed to the Supreme Court and the hearing of that appeal is now listed for January 2019. The High Court's request for a preliminary ruling remains pending before the CJEU.
- The DPC acted as lead reviewer in relation to 13 Binding Corporate Rules (BCRs) applications.
- A national survey carried out in May 2018 demonstrated a doubling of awareness of the GDPR in the SME sector from the same period in 2017. In May 2018, the results confirmed that over 90% of businesses were aware of the GDPR.
- DPC staff spoke and presented at events on almost **120 occasions**, including conferences, seminars, and presentations to individual organisations from a broad range of sectors.
- Our Twitter account, @DPCIreland, continued to show a significant growth rate, with followers up to **5,500** by 24 May, 2018. We also launched a DPC LinkedIn account in early 2018. Both our Twitter and LinkedIn accounts were used to raise awareness of the GDPR, as well as highlight the DPC's guidelines and tools published on www.dataprotection.ie and www.GDPRandYou.ie.

DPC staff spoke and presented at events on almost

120

occasions

5,500

Twitter followers

Contacts, Queries and Complaints

A key objective of the old office of the Data Protection Commissioner and of the new Data Protection Commission is the provision of a responsive and high quality information service to individuals and organisations regarding their rights and responsibilities under data protection legislation and the functions of the DPC.

The DPC's Information and Assessment Unit, which provides this public information helpdesk service, receives and responds to queries from individuals and organisations by means of email, online form, or by telephone. In addition, the Unit also engages with individuals and assesses concerns and complaints received in relation to potential infringements of these individuals' data protection rights.

Responding to queries

The period from 1 January 2018 to 24 May 2018 was an exceptionally busy time for our Information and Assessment Unit, particularly in the run up to the implementation of the General Data Protection Regulation (GDPR). During the five months up to 25 May, the Unit received almost 22,000 contacts comprising over 9,900 emails, 10,200 telephone calls, and approximately 1,800 items of correspondence via post. The month of May saw a significant increase in demand, with nearly 6,000 contacts made with the Unit in the month and an average of 270 contacts per working day.

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

Receiving and assessing complaints

From 1 January 2018 to 24 May 2018, nearly 1,050 complaints from individuals were received and examined by the DPC. This was very much in line with the number of complaints received by the DPC during the corresponding period of 2017. With the application of the GDPR it is expected that there will be an increase in the total number of complaints received for the full year of 2018.

In the case of complaints, an important function of the DPC is to provide individuals with the necessary assistance to enable them to resolve their data protection concerns directly with the organisation that has been controlling or processing their personal data. In many cases, concerns and complaints have been resolved in this way. In other cases, the DPC has engaged with the individual and organisation to address the complaint or facilitate an amicable resolution. In some further cases, depending on the nature of the matter, it has been necessary to initiate an investigation on foot of the complaint.

Preparation for the GDPR

Finally, a key DPC priority during the period from 1 January to 24 May 2018 was to continue to grow, prepare for, and enhance the services of the Information and Assessment Unit with the application of the GDPR. Over this period the team grew by 53% from 13 to 20 staff members and has worked to put in place new procedures, systems and information resources to better respond to the increasing volume of complaints and queries received and to continue to enhance the service provided to individuals and organisations.

Monitoring trends and promoting learning from queries and complaints

The DPC's information service also provides valuable insight into emerging data protection issues that are of concern to individuals and organisations. By monitoring the nature of queries and complaints received, the Information and Assessment Unit team assist the DPC in identifying trends and promoting learning amongst organisations about how best to comply with data protection legislation and protect the data protection rights of individuals.

During the period 1 January to 24 May 2018, in the run up to the implementation of the GDPR, the DPC identified a number of areas where additional information and guidance would enable organisations to better prepare for the GDPR. For example, requests from data controllers about the role of Data Protection Officers identified this topic as one of importance. This led to the DPC introducing guidance on the role of Data Protection Officers. Similarly, in response to queries from individuals in relation to how they should make access requests under the GDPR, guidance on this topic was developed and published on our website. This guidance contains a useful template to assist individuals in making an access request to an organisation and exercising their enhanced data protection rights under the GDPR.

Electronic Direct Marketing Complaints

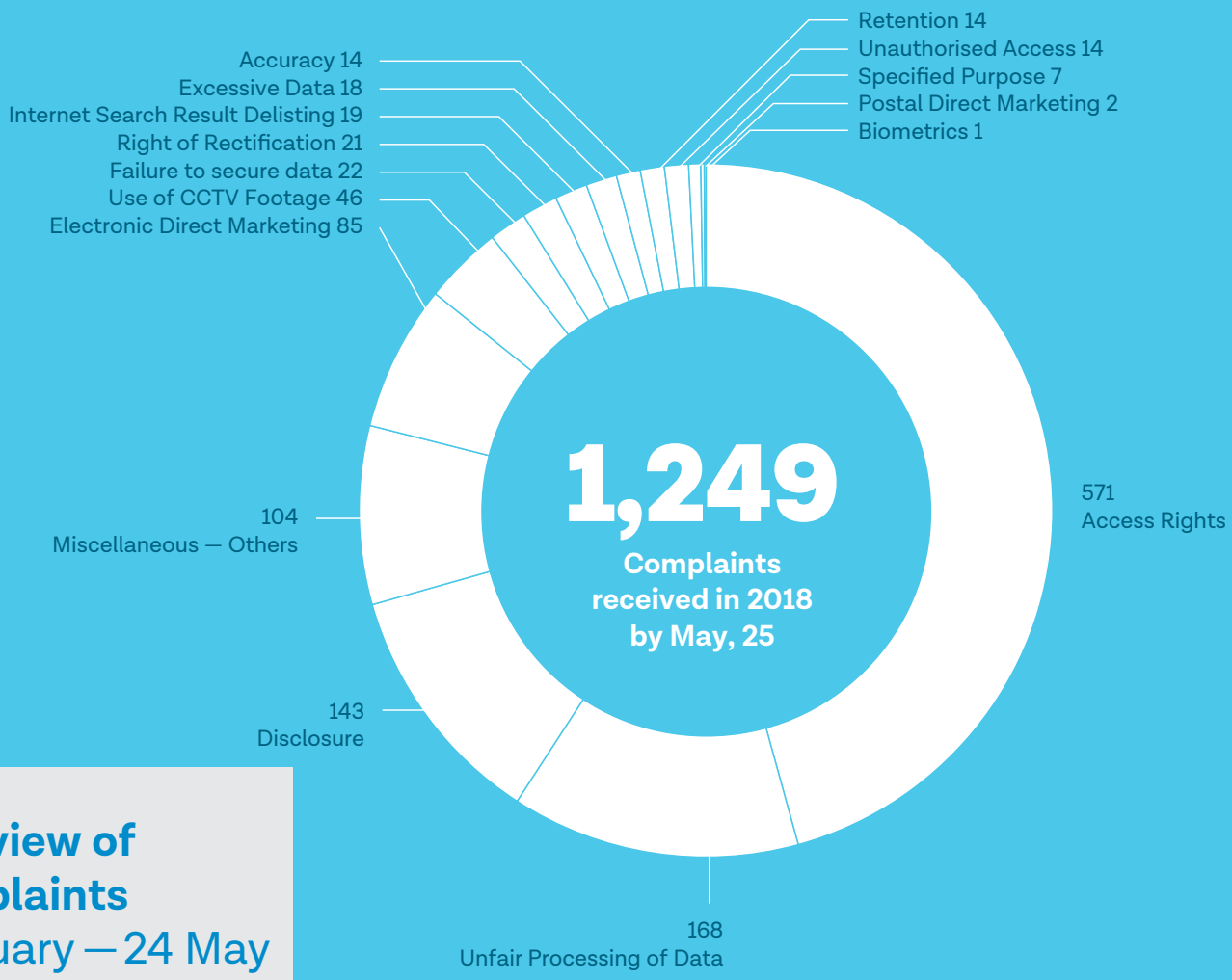
The DPC investigated 41 new complaints under the E-Privacy Regulations from 1 January — 24 May 2018 in respect of various forms of electronic direct marketing. (In 2017, the total number of new complaints investigated in this category for the whole year was 124). Of the 41 complaints investigated, 24 related to email marketing, 16 related to SMS (text message) marketing and one complaint related to telephone marketing.

The DPC completed 62 electronic direct marketing complaint investigations during this period. A number of these investigations concluded with successful District Court prosecutions by the DPC. In this regard, prosecutions were concluded during this period against three companies in respect of a total of 46 offences under the E-Privacy Regulations. These prosecutions resulted in convictions on four samples charges and the application of the Probation of Offenders Act in relation to three charges. The details of these prosecutions are set out in Appendix II.

Conclusion of Complaints

Under the Data Protection Acts 1988 and 2003, it was the statutory obligation of the DPC to attempt to amicably resolve complaints received from members of the public. Throughout the period 1 January to 24 May 2018, the vast majority of complaints were concluded amicably between the parties to the complaint without the necessity for issuing a formal decision under Section 10 of the Data Protection Acts 1988 and 2003. 12 decisions were issued under this provision of which nine fully upheld the complaint, one partially upheld the complaint and two rejected the complaint. A total of 1,046 complaints were concluded during this period. (Case studies in relation to these complaints are at Appendix II).

Breakdown of complaints by data protection issue



Overview of Complaints

1 January — 24 May

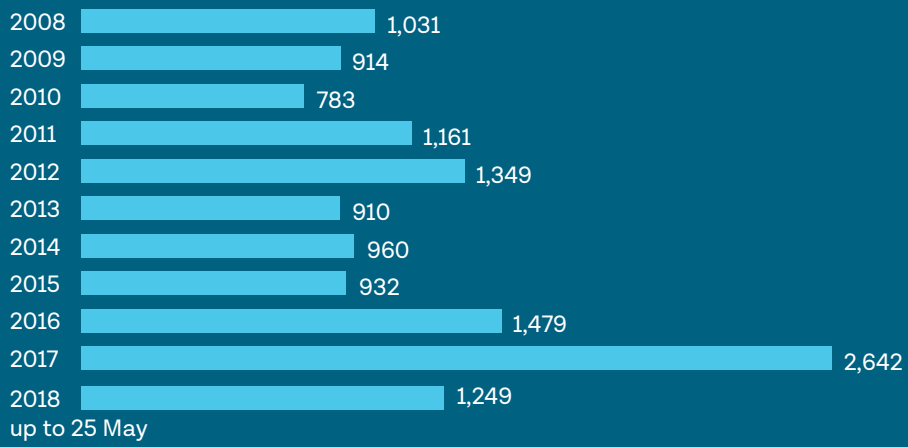
1,249

Complaints opened

1,046

Complaints concluded

Number of complaints received since 2008



Special Investigations

The DPC's Special Investigations Unit (SIU) was established in 2015 primarily to carry out investigations on its own initiative, as distinct from complaints-based investigations. This section of the report details some of the work undertaken by the SIU in the period under review.

Private Investigator Sector

Work continued in this period on the ongoing investigation into the private investigator sector and inspections were carried out by members of the SIU at the premises of two private investigators.

Letterkenny Circuit Court

In January 2018, the DPC's SIU was represented at a prosecution at Letterkenny Circuit Court at which the defendant, a former civil servant at the Department of Employment Affairs and Social Protection, was accused of a number of offences of receiving corrupt payments between 2008 and 2010 from two private investigators in exchange for supplying them with personal information held on the computer database of his then employer, the Department of Employment and Social Protection.
At the hearing, the defendant pleaded guilty to 12 sample counts out of a total of 41 charges relating to breaches of section 1(1) and (4) of the Prevention of Corruption Act, 1906 as amended by section 2 of the Prevention of Corruption Act, 2001. The Court sentenced the defendant to two years' imprisonment on each of the 12 counts to run concurrently with the final year suspended.

The DPC welcomed the outcome of this case, which followed separate investigations by An Garda Síochána and the DPC.

The Hospitals Sector

In 2017, the SIU opened an investigation to examine the processing of patient sensitive personal data in areas of hospitals in Ireland to which patients and the public have access. This investigation, which involved inspections at 20 hospitals, concentrated in particular on the circulation and journey of patient files in order to identify any shortcomings in terms of meeting the requirements of the Data Protection Acts 1988 and 2003 to keep personal data safe and secure and to have appropriate measures in place to prevent unauthorised access to, or disclosure of, personal data.

Drawing from the findings of the 20 hospital inspections, the SIU drew up an overall investigation report for dissemination to every hospital in the State. The report entitled "Data Protection Investigation in the Hospitals Sector" was published in May 2018. The primary purpose of this investigation report was to bring to the attention of every hospital in the State these matters of concern in relation to data protection compliance and to prompt them to examine whether any such issues were occurring or could occur in its facility and, if so, to implement the recommendations made in the report to remedy the situation.

The investigation report set out 14 main matters of concern. For each matter of concern, the report identified risks and set out recommendations to mitigate those risks. Across the 14 matters of concern, the report identified a total of 35 risks and it made 76 recommendations. The matters of concern that arose are set out in the following 14 categories were:

- Controls in Medical Records Libraries;
- Security;
- Storage of Patient Observation Charts in Hospital Ward Settings;
- Storage of Patient Charts in Trolley Bins in Ward Settings;
- Storage of Confidential Waste Paper Within the Hospital Setting;
- Disposal of Handover Lists and Patient Lists;
- Use of Fax Machines;
- Lack of Speech Privacy;
- Absence of Audit Trails;
- Raising Awareness of Data Protection in Hospitals;
- Consent for Research;
- The Processing of Private Health Insurance Information in Hospitals;
- Maternity Service Users; and
- Data Retention.

In disseminating the investigation report to the hospitals across the State, the SIU requested them to examine whether any or all of issues highlighted in the 14 matters of concern were occurring or could occur in their facility and, in doing so, to consider every part of the entire hospital campus as part of their examination. To assist hospitals in identifying the data protection risks relevant

to their facilities and to aid them in deciding the remedial actions they intend to take to mitigate those risks, a template data protection quality improvement plan was issued by the SIU with the investigation report.

Behind every hospital attendance is the creation and processing of patient registration forms, charts, scans and other documentation containing both personal data and sensitive personal data. Hospitals are, therefore, custodians of vast quantities of patient data. In many instances, no other organisation in the State holds as much sensitive personal data on some individuals. Data protection compliance goes to the very heart of the dignity of the patient while in a hospital setting and the processing of personal data is at the core of the treatment and medical care of every hospital patient. For these reasons in particular, the DPC called for all hospitals in the State to seriously reflect on the contents of the investigation report, and immediately set about identifying any data protection risks across their hospital campus and take appropriate steps to mitigate them.

Tusla Child and Family Agency

In March 2017, the SIU initiated an investigation to examine the governance by Tusla Child and Family Agency of personal data concerning child protection cases.

As reported in the DPC's Report 2017, this special investigation was initiated in March 2017 arising from information that came into the public domain in February 2017 regarding concerns relating to the handling of personal data and sensitive personal data at Tusla. The SIU completed its investigatory work in December 2017 and its findings (59 in total under 12 topic headings), were presented to Tusla in January 2018.

One of the main conclusions of the investigation was in the area of processing personal and sensitive personal data in the context of file management and record keeping. The DPC's SIU concluded that there had not been sufficient planning when Tusla was established in 2014 for a robust data governance strategy that brought together considerable volumes of casework and over 4,000 staff from three existing, but distinct agencies.

The following were among the other main findings of the investigation:

- It is critical that the casework management system deployed across all areas of Tusla generates a full and complete record of all casework material concerning each case in order to mitigate the risk that the system might give an inaccurate, incomplete or distorted view of each case. Evidence was identified in the investigation of multiple and overlapping volumes of individual case files where no complete 'master file' could be discerned and with no audit trail in relation to the handling of the file; and
- Existing links to the HSE in relation to office space, services and ICT systems featured prominently during the course of the inspections and the findings set out several issues of concern in that regard.

In presenting the findings of its investigation to Tusla, the SIU requested Tusla to present a plan of action within two months outlining how it planned to deal with the findings. Tusla submitted its action plan to the SIU in early April 2018. Having reviewed the action plan, the SIU submitted its observations to Tusla at the end of April 2018.

The Public Services Card (PSC)

Work continued during the period under review in relation to the special investigation of the PSC which was commenced in October 2017 and which was referred to in the 2017 Report. 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.

The investigation, which is split into modules, is ongoing and the preliminary findings, together with a number of request for further information in respect of the first module, were issued in August 2018 to the Department of Employment Affairs and Social Protection for comments and responses.

Data Breach Notifications

In the period 1 January to 24 May 2018, the DPC received 1,250 data breach notifications made under the Personal Data Breach Code of Practice — of which 52 cases (4%) were classified as non-breaches. Therefore, a total of 1,198 valid data security breaches were recorded by the DPC during this period.

This Code of Practice is not legally binding and does not apply to telecommunications and internet service providers, who have a legal obligation under Statutory Instrument 336 of 2011 to notify the DPC of a data security breach no later than 24 hours after initial discovery of the breach. The DPC received a total of 36 valid data breach notifications during this period in respect of the telecommunications sector.

As in other years, the highest category of data breaches reported under the Code of Practice were "Unauthorised Disclosures" and such breaches accounted for just under 59% of total data breach notifications received in the period 1 January to 24 May 2018.

Typical examples of data breaches include:

- inappropriate handling or disclosure of personal data e.g. improper disposal, third party access to personal data — either manually or online — and unauthorised access by an employee;
- loss of personal data held on smart devices, laptops, computers, USB keys, paper files; and
- network security compromise/website security breaches e.g. ransomware, hacking, phishing.

IT-related data breaches notified to the DPC are assigned to a dedicated Technical Audit team who review the actions taken by data controllers in response to such breaches and, where appropriate advise organisations on further measures to strengthen system security to ensure repeat of such IT-related breaches do not occur.

The tables below provide a breakdown of Data Breach Notifications received in the period 1 January to 24 May 2018.

Table 1: Number of Breach Notifications received in the period 1 January to 24 May 2018

Total Number of Breach Notifications Received	1250
Number considered as Non-breach	52
Number of Valid Breach Notifications	1198

Table 2: Previous Years Breach Notifications

Year	Number of Valid Breach Notifications
2014	2,188
2015	2,317
2016	2,224
2017	2,795
1 January to 24 May 2018	1,198

Technology-related breach investigations

Between 1 January and 24 May 2018, 16 technology-related data breaches were investigated. Of these, seven involved a data controller's usage of cloud-based environments as offered by a variety of cloud service providers. This represents a continuation of trends identified in 2017.

The majority of these data breaches involved:

- Overreliance on data processors for the implementation of appropriate security measures including for example, failure to modify the default security settings offered by cloud service providers which resulted in unauthorised access to personal data;
- Insufficient awareness of security protocols which may be implemented as part of the use of cloud-based environments for personal data processing including for example, failure to implement two-factor authentication;
- Failure to appropriately scope and implement security measures relating to the organisation's specific security requirements including for example, seeking formal assurances from data processors that such measures were implemented;
- Poor governance and control structures including for example, failure to have in place appropriate data processing agreements that ensure the delineation of data processor obligations in respect of the security of processing; and/or
- An absence of follow-up procedures to ensure security measures are appropriate and up to date including for example, periodic reviews of security measures and the configuration of those security measures.

In addition, the technology-related data breaches also demonstrated trends of which data controllers should be aware. It is therefore recommended that data controllers employing cloud-based environments as part of their processing of personal data should consider the following in respect of their use of such services:
Data controllers should themselves determine the security measures which are appropriate for application in respect of their processing of personal data;

- Data controllers should review security best practice information made available by their cloud service providers;
- Default security settings should not be relied upon and all vendor-provided security measures should be reviewed and amended as appropriate; and
- Data controllers should review their access control and authentication procedures to ensure appropriate safeguards are in place such that:
  - users have the minimum appropriate permissions to perform their duties;
  - strong password policies are enforced;
  - steps are taken to ensure only authorised users can access cloud-based environments, with appropriate controls in place to mitigate the risk of an attack;
  - regular reviews of user permissions are conducted and accounts that are no longer required are
    removed;
  - personal data that is transmitted over a network or stored at rest is secured; and
  - reviews are conducted of intrusion prevention and detection measures and audit and log trails in conjunction with monitoring to ensure the rapid detection of suspicious behaviour.

In general, while many organisations put in place effective ICT security measures, we identified that data controllers, in particular SMEs, do not take proactive steps to review these measures or to train staff to ensure awareness of evolving threats. We therefore recommend data controllers implement periodic reviews of ICT security measures and design and implement comprehensive training plans for employees, supported by refresher training and awareness programmes, to mitigate the risks encountered in the use of cloud-based environments.

Multinationals and Technology

Preparing for the GDPR

Supervision of the personal data processing activities of multinational companies in Ireland continued as a key DPC priority. Work was also prioritised to prepare the DPC to assume its role of Lead EU Supervisory Authority for those multinational companies who have their "main establishment" in Ireland under the GDPR "One-Stop-Shop" model.

The DPC's GDPR engagement with multinational companies focused predominantly on large-scale personal data processing of global multinational companies with EU headquarters located in Ireland, such as Facebook, LinkedIn, Google, Microsoft, Twitter, Oath EMEA, Ancestry and SurveyMonkey. These engagements typically consisted of companies presenting their GDPR-readiness programmes and seeking our observations on the application of the GDPR to their proposed policies, products and services.

Based on the information provided to us by multinational companies during this engagement, we provided observations on the implementation of GDPR obligations such as accountability, risk management, data protection by design and default, transparency, the use of appropriate legal basis, updated consent mechanisms and implementation of user rights.

Much of the DPC engagement with multinational companies in this period focussed on the compliance with key GDPR concepts, including the importance of:

- "clear and plain" information about processing operations of personal data and the requirements of Articles 12-14 of the GDPR;
- support for data subjects rights being facilitated and controls and information relating to such controls being clear and effective;
- risk management and the use of Data Protection Impact Assessments (DPIAs) to ensure proportionate, risk-mitigated and secure processing;
- accurate and effectively implemented retention policies and practises;
- clarity for data subjects on the extent, purpose, scope and nature of personal data sharing and third party personal data access;
- the interaction of the GDPR and the ePrivacy Regulations (S.I. 336 of 2011) in particular in relation to cookie storage and handling;
- providing the right to object to data subjects in appropriate instances including where processing is based on the "legitimate interests" of a controller, where a data subject receives direct marketing etc.;
- undertaking international transfers to third countries only with a lawful basis and ensuring adequate oversight, safeguards and transparency in this context;
- identifying minors and other data subjects as "vulnerable" data subjects and accordingly, affording additional or special protection to the processing of their personal data (including in relation to collection of consent from minors); and
- having an effective, expert, properly resourced and communicative Data Protection Officer (DPO), with no conflicts of interest and who has the ability to independently perform his or her duties while reporting to and being supported by senior management.

Our engagement with technology-based multinational companies achieved some significant results with some organisations altering and updating their approach to GDPR compliance and re-presenting their proposals to us.

Examples included:

- one company who proposed to obtain consent from a data subject to a number of processing purposes at the same time, updated their approach to separate the consents for each processing purpose thereby providing the user with ability to withdraw his or her consent to each processing purpose;
- a number of companies provided more detailed information to their users in respect of the lawful basis on which their processing purposes were based pursuant to Article 13(1)(c) and 14(1)(c) GDPR. The purpose of these changes were to assist users of the relevant services to better understand how to exercise their rights;
- proposed interfaces with users were amended to present the information more clearly to users on mobile devices; and
- some companies re-considered in what instances consent would be sought from minors or explicit consent would be sought from users in respect of the processing of special categories of personal data and for what purposes special category data would be used.

Supervision of Facebook Ireland

Apps access to user data

The nature and extent of third party apps access to Facebook's user data came under the spotlight in early 2018. The misuse of personal data by apps on the Facebook platform poses significant data protection risks to users. The DPC continues to actively supervise both the lookback review of third party apps and the wider review of its third party app platform currently being conducted by Facebook. In particular, we are focusing on Facebook's ability to govern and oversee in a comprehensive and effective manner the activities of app developers, especially their capacity to swiftly identify and respond to "bad actors" and misuse of personal data.

The controversy surrounding the use of Facebook user data by third parties also highlighted the need for better user awareness on how to take control of settings available on social media platforms that curtail the collection and use of user data. In response we published guidance "Tailoring your Social Media Privacy and Advertising Preferences" to assist individuals in safeguarding their personal data when using social media.

Facial Recognition

During engagement with Facebook on GDPR-readiness, Facebook informed the DPC that facial recognition for users would be trialled in specified EU countries and subsequently rolled-out across the EU. The DPC reminded Facebook that facial recognition services are a form of processing of biometric data which, under the GDPR, is a special category of personal data. The DPC noted that the processing of biometric data was therefore subject to the protection of special categories of data as specified in the GDPR, and that Facebook should take into account the concerns of the DPC and other EU data protection authorities regarding facial recognition technology as expressed in the context of the DPC's audit of Facebook in 2011-2012. The outcome of that audit contributed to the deactivation of Facebook's facial recognition technology for users in the EU at that time.

While explicit consent of the data subject is required as a lawful basis for all users who choose to "opt-in" to the use of such technology, compliance with the GDPR extends beyond mere compliance with Article 9 of the GDPR. The broader compliance standard extends to account default settings, transparency obligations, the rights of users — and non-users or users who have not opted-in — and the scope and nature of the technical elements of the processing of biometric data.

The DPC's examination of Facebook's facial recognition facility is ongoing.

Supervision of LinkedIn Ireland

LinkedIn Audit

The DPC concluded its audit of LinkedIn Ireland Unlimited Company (LinkedIn) in respect of its processing of personal data following an investigation of a complaint notified to the DPC by a non-LinkedIn user. The complaint concerned LinkedIn's obtaining and use of the complainant's email address for the purpose of targeted advertising on the Facebook Platform. Our investigation identified that LinkedIn Corporation (LinkedIn Corp) in the U.S., LinkedIn Ireland's data processor, had processed hashed email addresses of approximately 18 million non-LinkedIn members and targeted these individuals on the Facebook Platform with the absence of instruction from the data controller (i.e. LinkedIn Ireland), as is required pursuant to Section 2C(3)(a) of the Acts.

The complaint was ultimately amicably resolved, with LinkedIn implementing a number of immediate actions to cease the processing of user data for the purposes that gave rise to the complaint.

However, following on from this complaint, the DPC was concerned with the wider systemic issues identified and an audit was commenced to verify that LinkedIn had in place appropriate technical security and organisational measures, particularly for its processing of non-member data and its retention of such data. The audit identified that LinkedIn Corp was undertaking the pre-computation of a suggested professional network for non-LinkedIn members. As a result of the findings of our audit, LinkedIn Corp was instructed by LinkedIn Ireland, as data controller of EU user data, to cease pre-compute processing and to delete all personal data associated with such processing prior to 25 May 2018.

Supervision of WhatsApp

We continued to supervise WhatsApp's cooperation with Facebook to ensure that the commitment made by WhatsApp to DPC Ireland in 2016 to pause data sharing for product enhancement, ad serving and safety and security purposes on a Data Controller to Data Controller basis from WhatsApp to Facebook, remains in place. Data sharing for these purposes will not occur prior to further engagement with DPC at which time we will assess in detail the compliance with the GDPR of any such proposal.

Supervision of Yahoo/Oath

Yahoo Breach Report

Work concluded on our investigation of a data breach concerning Yahoo! EMEA Limited ("Yahoo"), since renamed Oath (EMEA) Limited. The breach, reported to the DPC in September 2016, involved the unauthorised copying and taking by one or more third parties of material contained in approximately 500 million user accounts from Yahoo! Inc. infrastructure in 2014.

The findings made by the DPC included the following:

- Yahoo's oversight of the data processing operations performed by its data processor did not meet the standard required by EU data protection law as given effect or further effect in Irish law;
- Yahoo relied on global policies which defined the appropriate technical security and organisational measures implemented by Yahoo and those policies did not adequately take into account Yahoo's obligations under applicable data protection law; and
- Yahoo did not take sufficient reasonable steps to ensure that the data processor it engaged complied with appropriate technical security and organisational measures as required by applicable data protection law.

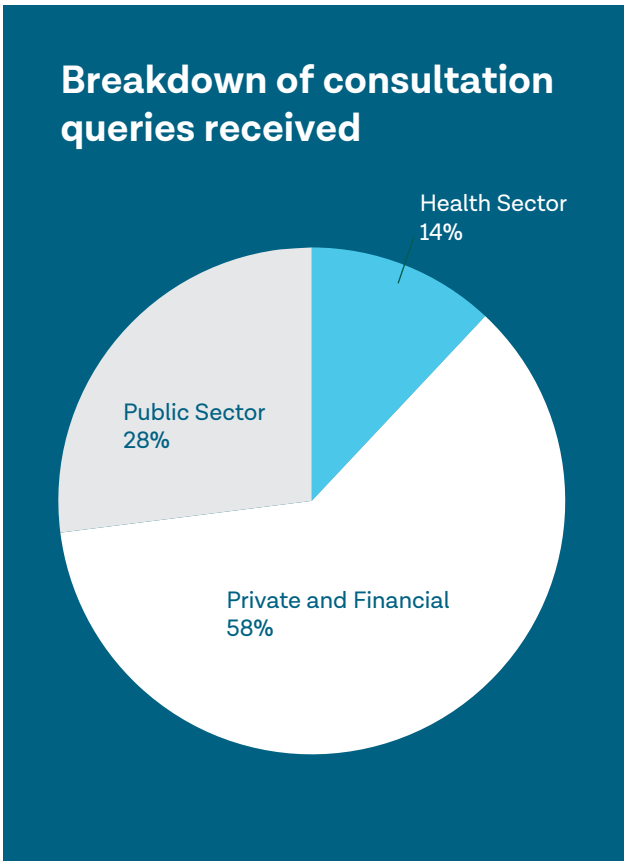
Based on its findings, the DPC notified Yahoo that it is required to take specified and mandatory actions to bring its data processing into compliance with EU data protection law and as given effect or further effect in Irish law.

The actions Yahoo is required to take include that it should ensure all data protection policies that it uses and implements take account of the applicable data protection law and that such policies are reviewed and updated at defined regular intervals. Yahoo was also instructed to update its data processing contracts and procedures associated with such contracts to comply with applicable data protection law. The DPC also directed Yahoo to monitor any data processors which it engages for compliance with data protection law on an ongoing basis in accordance its obligations under applicable data protection law.

Consultation

2018 General Queries (pre 25 May 2018)

The DPC's Consultation Unit received 503 general queries in the period 1 January to 24 May 2018. (These figures do not include consultations with multinational companies). The breakdown of the general consultation queries mirrors the trend identified in 2017 where over half of queries received came from the private sector. This reflects a growing cognisance of data protection by small to medium sized businesses who were targeted as part of the DPC's intensive GDPR awareness campaign which was instrumental in achieving over 90% awareness of the GDPR in the SME sector. The complexity and nature of queries received suggested a level of awareness and eagerness to meet the requirements of the GDPR among both data controllers and data processors across all sectors.



Engagement

In the period 1 January to 24 May 2018, the Consultation Unit continued to engage with key stakeholders across the public and private sectors to assist organisations in their preparations for the GDPR. This engagement included reaching out to public sector bodies, industry representative bodies, relevant Government Departments, and our European counterparts and colleagues as well as meeting with individual organisations on a consultative basis in relation to their GDPR preparations. In driving awareness of the GDPR and providing guidance on its application, our key message was that the 25 May 2018 date was not the endgame and that compliance with the data protection legal framework will be an ongoing and evolving issue for data controllers and processors.

Some of the organisations we engaged with in the first half of 2018 included:

Public Sector

Sligo Local Enterprise Office — GDPR readiness forum

Tusla/Department of Children and Youth Affairs — Data sharing

Department of Taoiseach — Data Protection Forum

Local Government Management Agency (LGMA)

Adoption Authority of Ireland — Social Work Practitioners

Health Sector

HSE / Healthlink — GDPR preparedness

Department of Health — Guidance in terms of drafting Health Sector Regulations

Irish College of General Practitioners — Guidance

Southdoc — GDPR readiness forum

Social Care Ireland

HSE — Data Protection Readiness update

HIQA — Guidance on a Data Quality Framework for health and social care

Private/Financial Sector

AIB — GDPR preparedness

Permanent TSB — GDPR preparedness

Central Bank of Ireland — GDPR preparedness

Bank of Ireland — GDPR preparedness

Banking and Payments Federation Ireland

European Association of Communications Directors

International Association of Privacy Practitioners Knowledge Net briefing on the GDPR

World Rugby — GDPR readiness

Sports Federations — GDPR readiness Forum

Health and Safety Review — Annual Conference

IBEC OSH Group — GDPR Webinar

Independent Holiday Hostels of Ireland — GDPR readiness

Charity/Voluntary Sector

Patient Focus — Data Protection Policy

Dochas — GDPR readiness forum

Kerry Volunteer Centre

Nursing Homes Ireland — GDPR readiness conference

Legislative Observations

Legislative observations were provided on the following matters:

Data Sharing and Governance Bill 2018

Data Protection Bill 2018

Disabled Driver and Disabled Passengers Fuel Grant draft Regulations

4th Anti Money Laundering Directive and Beneficial Owners Register draft Regulations.

Guidance to Government departments and public bodies on the drafting of regulations to restrict the rights of data subjects the Data Protection Bill on enactment.

Data Protection Audits

In the period from 1 January to 24 May 2018, 23 audits/inspections were carried out (the list of organisations audited can be viewed in Appendix 1). The aim of all audits and inspections is to check for compliance with data protection legislation and to assist the data controller or data processor in achieving best practice in terms of its data processing operations. Priorities and targets for audit are selected by considering matters such as the amount and type of personal data processed by the organisation concerned as well as the number and nature of queries, complaints and breach notifications that we receive.

Our target selection in 2018 was, as in previous years, strategic and designed to ensure a balance between the need to monitor areas of high-risk, large scale processing and to react to trends detected both externally and internally, identifying areas or issues suitable for further investigation through the audit mechanism.

The DPC, in response to specific complaints or allegations received, may also carry out audits and during the period under review this led to a series of audits of lettings agents. These audits highlighted the fact that excessive amounts of personal data is being collected from prospective tenants.

At the end of 2017, the DPC audited the recently established Credit Register. In line with the supervisory functions afforded to the DPC in the Credit Reporting Act 2013, we carried out further examinations in 2018 of the functions and workings of the Credit Register in our focused audits of Bank of Ireland and Drumcondra Credit Union.

Lettings Agents

In 2017, the DPC received a number of complaints with regard to the level of personal data being requested from prospective tenants by lettings agents and landlords operating in the residential lettings sector. In particular, the queries/complaints highlighted to the DPC that excessive personal information, including photo identities and PPSNs are requested from prospective tenants prior to them being offered a lease.

Both the Data Protection Acts 1988 and 2003 and the GDPR require organisations collecting personal data only to seek personal information for which they have a specific justification for requesting. An organisation has no business collecting or keeping personal information that it does not specifically need, 'just in case' a use can be found for the data in the future.

The collection of photo identities in the lettings process prior to a lease being agreed was raised as a concern by individuals contacting this office. The DPC can see no basis for requiring photo identity at application stage (pre-tenancy) in the absence of any legitimate business reason requiring same. The DPC considers that landlords and lettings agents may cite legitimate reasons for requesting and retaining the photo identity of a tenant renting their property, once the contract is signed.

Landlords, or their agents, should not seek PPSNs during the initial phase of the lettings process and should only do so when the lease is being agreed. There is a statutory basis for a landlord (or their lettings agent acting on their behalf) to seek the PPSNs of their tenants under the Residential Tenancies Act 2004 and section 11 of the Social Welfare (Miscellaneous Provisions) Act 2004. This information is required for registration with the Private Residential Tenancy Board (PRTB). However, a landlord (or their lettings agent) is authorised to use the PPSNs of tenants for registration with the PRTB only. No other use should be made of the PPSNs and they must be kept confidential.

The DPC considers that it is reasonable for a landlord or lettings agent to request supporting documentation to confirm a prospective tenant's capacity to pay rent. In relation to bank statements, the DPC is of the opinion that providing details of the nature of specific transactions will generally not be necessary, and therefore removing the narrative of transactions and providing the running balances is sufficient to demonstrate capacity to pay. Requests for details in relation to employment/salary may also be reasonable to confirm capacity to pay rent. However, requesting the bank details of a prospective tenant for the purpose of lodging the rent payment, or putting utility bills into the tenant's name, prior to a lease being agreed, is a practice of concern from a data protection
perspective.

Retention of personal data

The Data Protection Acts 1988 and 2003, and now the GDPR, provide that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. In determining appropriate retention periods for personal information, data control-

lers must have due regard for any statutory obligations. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

The DPC advises that the personal data of all unsuccessful applicants for rental properties should be disposed of securely. In the case of the manual application forms, these should be shredded shortly after the letting has been closed, e.g., on a weekly basis. In respect of email or online applications, these should be permanently deleted shortly after the letting has been closed.

In relation to successful applicants who become tenants, the DPC is cognisant that personal data submitted in connection with their application is required to be held for the duration of the tenancy. It is recommended that a retention period is drawn up by landlords/lettings agents to ensure personal data in relation to a tenancy is disposed of in a secure manner after a specified time period once a tenancy has ceased.

Audit Findings

Themes identified in the 2018 audits are set out below.

1. Retention of electronic and manual data

Both the Data Protection Acts 1988 and 2003 and the GDPR provide that organisations should not retain personal data for longer than is necessary for the purpose it was collected. Our audits continue to find that data controllers routinely shred manual paper files due to storage issues. However, this is not always the case with computerised data, where vast amounts of personal data can be stored relatively cheaply. It is imperative that data controllers ensure that when implementing data retention policies, the retention period applies equally to both manual and computerised data.

2. CCTV policies

Recognisable images captured by CCTV systems are considered to be personal data. Many organisations and SMEs legitimately use CCTV for security purposes where there are issues of theft. However, it is best practise to have a CCTV policy to ensure full clarity on its purposes and uses. It is difficult to justify the use of CCTV in some circumstances where its intended use is not stated in a policy. It is important to consider the following when drafting a CCTV policy:

- What the system will be used for?; for example, security;
- Justification for the use of CCTV — whether it is proportionate;
- Will CCTV be used other than for security purposes?;
- Where the cameras are located;
- Who has access to the CCTV system, including any third parties?;
- Clear signage in place alerting individuals to the use of CCTV on a premises;
- How an individual can make an access request for their images captured on CCTV;
- What is the retention period for images captured?;
- How will images be securely destroyed?;
- How requests for footage from An Garda Síochána will be dealt with.

3. Cookies

When internet users visit a website, cookies may be placed on their terminal equipment by the website when a user consents to them. When the GDPR came into application in May 2018 references to consent in the current SI or ePrivacy directive to 95/46/EC are replaced with references to GDPR consent. Such consent is between a user and an accountable data controller — usually the website owner but also sometimes others that are permitted to make use of parts of the website. Under the E-Privacy Regulations (S.I. 336 of 2011), the minimum requirement is that clear and comprehensive communication to the user as to what purposes he/she is being asked to consent to in terms of cookies usage and a means of giving or refusing consent is required. Under GDPR conditions for consent, a user can also withdraw it. In practical terms, data controllers who place cookies on their user's equipment or browsers should request consent in a manner which is clearly distinguishable from the other matters and purposes, in an intelligible and easily accessible form, using clear and plain language. The onus is on the controller to be able to demonstrate that the user has provided that consent.

4. Collection of PPSN

Data controllers can legitimately seek a PPSN from an individual in limited circumstances. Common examples are when an employee starts a job with a new employer, the new employee's PPSN is required for tax purposes; or, when a child starts school, the school is required to transmit the PPSN of all children attending the school to the Department of Education and Skills. However, the timing of a request for a PPSN is critical to the legitimacy of seeking such personal data. A PPSN should not be sought before it is actually required. For example, in schools, a PPSN should not be sought at pre-enrolment stage; a PPSN is only required if the child takes up the offer of a place and attends school. Equally, in an employment context, a PPSN should not be sought at the application stage as it will only be required if the applicant who is offered employment takes up the position.

5. Data Sharing Agreements

A key finding across a number of the audits carried out by the DPC is the need for organisations to review all information sharing agreements and protocols they may have in place. Post 25 May these need to be in compliance with the GDPR and the Data Protection Act 2018.

In response to findings such as these, the DPC makes best-practice recommendations and provides immediate direction to an organisation to take a particular action. These sample findings equally apply under the relevant articles of the GDPR.

Legal

Overview

The DPC's centralised legal unit was established in 2016. The legal unit operates horizontally within the DPC and is responsible for legal oversight and the provision of internal legal advice and support across all area of the DPC's functions, as well as 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 in relation to the applicable legal frameworks, legal developments and the performance of the DPC's functions at national and EU levels. In addition to the centralised unit, the DPC has further legal professionals, as well as staff with legal qualifications who operate within all of the DPC's functional areas. Specialist legal recruitment continued during the period under review with the addition of further senior legal advisers as well as legal researchers to the staff of the DPC.

Litigation involving the DPC

During the period from 1 January 2018 to 24 May 2018, judgment was delivered in the following proceedings to which the Data Protection Commissioner was a party:

An appeal to the High Court in the case of *Savage v Data Protection Commissioner* [2018 IEHC 122]

This case originated in a complaint made to the DPC about Google and its refusal to delist a link to a web page (for a discussion forum). The complainant had requested that Google remove the link in question from search results returned by a Google search against the complainant's name. The DPC's decision was that there had been no contravention of the Data Protection Acts 1988 and 2003 as the link to the web page was accurate in that it represented an opinion — about the data subject that was expressed by a user of the discussion forum — rather than a verified fact. The Circuit Court upheld the data subject's appeal on the basis that the link to the webpage bore the appearance of a verified fact and that therefore it was not accurate because it was not clear from the link that the original poster was expressing their opinion. Both the DPC and Google Ireland Limited (which was a Notice party to the Circuit Court appeal) separately appealed the Circuit Court judgment. The High Court appeals were heard together during May 2017. Judgment was delivered on 9 February 2018. In that judgment the Court overturned the Circuit Court judgment, finding that the Circuit Court had erred in not considering the underlying article to which the link in question related. If the Circuit Court had done so, it could not have come to the conclusion that the link was inaccurate data, factually incorrect or had the appearance of fact.

An appeal to the High Court in the case of *Peter Nowak v Data Protection Commissioner and Institute of Chartered Accountants in Ireland* [2018 IEHC 118]

This case originated in a complaint from Mr. Nowak, a trainee accountant, who failed an open book examination set by the Institute of Chartered Accountants of Ireland (CAI), in autumn 2009. He later sought access to his examination script which CAI refused on the ground that it did not contain his personal data. Mr. Nowak complained to the Commissioner who took the position that the examination script was not personal data and therefore refused to investigate the complaint, dismissing it in accordance with Section 10(1)(b)(i) of the Data Protection Acts 1988 and 2003 which concerns frivolous or vexatious complaints. In a separate set of

proceedings, Mr Nowak appealed the DPC's decision to the Circuit Court, the High Court and the Court of Appeal which each in turn upheld the position taken by the Commissioner and dismissed the relevant appeal. Mr Nowak was subsequently granted leave to appeal to the Supreme Court which referred the question of whether the examination script in question constituted personal data to the CJEU. The Supreme Court also held that there was a right to appeal against a decision of the DPC not to investigate a complaint. In its judgment of 20 December 2017, the CJEU ruled that the written answers submitted by a candidate at a professional examination, and any comments made by an examiner with respect to those answers, constitute personal data. (For a summary of this judgment see the 2017 Report of the Data Protection Commissioner).

The proceedings against CAI concerned a separate, but related complaint to the one described above. In his complaint to the DPC, Mr Nowak sought access to his original CAI examination script, asserting that the right of access under Section 4 of the Data Protection Acts 1988 and 2003 entitled a data subject to access their personal data in its original form. While the decision of the DPC (declining to investigate this complaint) had been appealed to the Circuit Court in 2014, the Court had not dealt with this particular issue and had simply upheld the decision of the DPC not to investigate the complaint. Mr Nowak appealed that Circuit Court decision to the High Court. The parties subsequently agreed that rather than remitting the question at issue (of whether the right of access involved the right to access personal data in its original form) to the Circuit Court, the High Court could instead determine this issue. The High Court in its judgment of 26 February 2018 held that the obligation on a data controller in relation to the right of access of a data subject was to communicate the relevant information (the personal data) not in its original form but rather in an "intelligible form" to the data subject. Prima facie this leaves it to the data controller to decide in what material form the data is communicated as long as it is sufficient to allow the data subject to become aware of the data and to check that they are accurate and processed in compliance with the Data Protection Directive so that the person may, where relevant, exercise their data protection rights. This did not extend to an obligation on the data controller to provide the data in its original material form or, in the case of a document, to provide the original of that document.

An appeal to the High Court in the case of *Peter Nowak v Data Protection Commissioner and Price Waterhouse Coopers* [2018 IEHC 117]

These proceedings concerned a complaint which had been made to the DPC by Mr Nowak against his former employer, Pricewaterhouse Coopers ("PWC") alleging that information contained in a memorandum prepared by PWC and submitted to the Chartered Accountants' Regulatory Board ("CARB") constituted Mr Nowak's personal data. The background to this related to a separate complaint which had been made by Mr Nowak to CARB against PWC alleging non-compliance by PWC with accounting and auditing standards in respect of two audits in which Mr Nowak had been involved in his previous role as a trainee accountant with PWC. PWC responded to CARB addressing the two complaints by letter and enclosing a memorandum. Mr Nowak then sought access to the memorandum on the basis that it was his personal data — which PWC disagreed with. Mr Nowak then made a complaint to the DPC claiming that the memorandum contained his personal data because it related to his complaint and allegations against PWC as well as the audit work that he had carried out as an employee of PWC. Following an on-site inspection of the material in the memorandum by an officer of the DPC, the DPC informed Mr Nowak in writing that there was no personal data relating to him contained in the memorandum and that he was not referred to in any way in the material. Upon appeal of the decision to the Circuit Court, the Court found that the DPC's decision that the material in dispute was not personal data was a reasonable one. That decision was then appealed to the High Court. During the hearing, the trial judge inspected the material in question. The Court held that the documents in question did not contain any data of a personal nature relating to Mr Nowak and did not refer to him in any way. The Court held that there appeared to be nothing in the material that related to Mr Nowak as an identified or identifiable natural person which engaged his right to privacy or which could in any meaningful way be amenable to the rights of objection, rectification or erasure under the Data Protection Acts 1988 and 2003. Noting that it was not for the Court to place itself in the shoes of the DPC or reconsider the matter de novo but rather to determine whether an error of law had been made by Circuit Court, the Court found no error of law in the Circuit Court judgment and dismissed Mr Nowak's appeal.

A complaint to the Equality Tribunal (now the Workplace Relations Commission) in the case of *A Separated Father v Data Protection Commissioner* [Equal Status Acts 2000-2012 Decision No. Dec-S2018-008]

This complaint to the Equality Tribunal related to a decision by the DPC not to investigate a complaint made to the DPC concerning the alleged unlawful disclosure of the complainant's personal data (in the form of an affidavit) by an authority to a school. The complainant complained that the release of the affidavit amounted to a contravention of the in camera rule in the context of court proceedings. An officer of the DPC responded to the complainant indicating that the question of the release of the affidavit and the alleged contravention of the in camera rule was a matter for the Court rather than the DPC. The complainant alleged that the decision of the DPC in this regard constituted discrimination against him by the DPC on the ground of marital status, arising from his status as a separated father. A preliminary issue arose in the case concerning the jurisdiction of the adjudication officer of the Equality Tribunal to determine a complaint in relation to a statutory decision-making body such as the DPC. In this context, the principle of judicial immunity was considered by the adjudication officer. In a decision of 10 April 2018, the adjudication officer decided that, as the services of the DPC are available to the public generally, it is subject to complaint under the Equal Status Acts unless bona fide exercising its quasi-judicial functions. In this case, an officer of the DPC had concluded that there were no grounds of investigation. The adjudication officer noted that there was no suggestion that the DPC had refused to investigate the complainant's complaint without any consideration of it or any other mal fides on the DPC's part that might serve to lift the protection of judicial immunity. In the circumstances, the adjudication officer considered that the DPC was entitled to judicial immunity and she therefore did not have jurisdiction to hear the complaint regardless of its merits.

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 Court of Justice of the European Union (CJEU) in relation to the validity of "standard contractual clauses" (SCCs). SCCs are a mechanism, established by a number of EU Commission decisions, under which, at present, personal data can be transferred from the EU to the US. The 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 to US personal data transfer regime). The CJEU ruled that this procedure (involving seeking a reference to the CJEU) must be followed by an EU data protection authority where a complaint which is made by a data subject concerning an EU instrument, such as an EU Commission decision, is considered by the EU data protection authority to be well founded.

(1) Background

The proceedings taken by the 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., his personal data was then being accessed (or was at risk of being accessed) unlawfully by US state security agencies. Mr Schrems' concerns arose in light of the disclosures by Edward Snowden regarding certain programmes said to be operated by the US National Security Agency, most notably a programme called "PRISM". The (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 data protection authority which involves a claim that an EU Commission decision is incompatible with protection of privacy and fundamental rights and freedoms, the relevant data protection authority must examine that complaint even though the data protection authority cannot itself set aside or disapply that decision. The CJEU ruled that if the data protection authority considers the complaint

to be well founded, then it must engage in legal proceedings before the national Court and, if the national Court shares those doubts as to the validity of the EU Commission decision, the national Court must then make a reference to the CJEU for a preliminary ruling on the validity of the EU Commission decision in question. As noted above, the CJEU in its judgment of 6 October 2015 also struck down the EU Commission decision which underpinned the Safe
Harbour EU to US data transfer regime.

(3) 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 will 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 to be joined as amicus curiae ("friends of the court") to the proceedings and the Court ruled four of those ten parties (the US Government, BSA The Software Alliance, Digital Europe and EPIC (Electronic Privacy Information Centre)) should be joined as amici.

The hearing of the proceedings before Ms Justice Costello in the Irish High Court (Commercial Division) took place over 21 days in February and March 2017 with judgment being reserved at the conclusion of the hearing. In summary, legal submissions were made on behalf of: (i) each of the parties, being the 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 5 expert witnesses on US law, as follows:

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

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

(5) Judgment of the High Court

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

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

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

had been made in the judgment of 3 October 2017. The Court reserved its judgment on these matters.

(6) Questions to be referred to the CJEU

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

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

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

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

(7) Appeal to the Supreme Court

On 11 May 2018, Facebook lodged an appeal, and applied for leave to appeal to the Supreme Court, against the judgments of 3 October 2017, the revised judgment of 12 April 2018 and the judgment of 2 May 2018 refusing a stay. Facebook's application for leave to appeal to the Supreme Court was heard on 17 July 2018. In a judgment delivered on 31 July 2018, the Supreme Court granted leave to Facebook allowing it to bring its appeal in the Supreme Court but directing that the refinement of the specific issues for determination in the appeal should be dealt with by way of case management ahead of the full hearing in the Supreme Court. The hearing of the Supreme Court appeal has been fixed for 21 January 2019. 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, together with 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.

Binding Corporate Rules

Binding Corporate Rules (BCRs) were introduced following discussions at Article 29 Working Party in response to the need of organisations to have a global approach to data protection where many organisations consisted of several subsidiaries located around the globe. 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 signing of contracts such as standard contractual clauses or approvals by several DPAs. The GDPR outlines in Article 47 how BCR's can continue to be used as an appropriate safeguard to legitimise transfers to Third Countries.

During the period 1 January — 24 May 2018 the DPC acted as lead reviewer in relation to 13 BCR applications. Four of these applications were given final approval by the DPC, namely:

- Workday Limited;
- Docusign Limited;
- VMware International Limited; and
- Twilio Ireland Limited.

We assisted other DPA's as co-reviewer on five BCR's in this period and four have been approved by the DPA's concerned, namely:

- AGCO (Bavarian DPA);
- Ernst and Young (ICO);
- Deloitte (ICO); and
- ISS Group (Danish DPA).

It is envisaged that with the recognition of BCRs as a tool to transfer data in the GDPR (Article 47) and the introduction of a one stop shop mechanism that there will be an increase in such applications to this office from 25 May 2018.

DPC's Internal GDPR Readiness Programme

Similar to many other Data Protection Authorities across Europe, the DPC's own GDPR Readiness Programme continued to be a priority initiative during the period 1 January — 24 May 2018.

The primary objective of this Programme was to best prepare the office to deliver the range of new and expanded functions as a regulator under the GDPR, Law Enforcement Directive, Data Protection Act 2018 and proposed ePrivacy Regulation.

The Programme comprised of 28 different workstreams focussed on readiness activities related to the office's staff, processes, systems, structures and technology, as well as enhancing external readiness / awareness of the new legislation.

Each workstream was led by a senior DPC staff member and supported by staff across the organisation. The Programme was governed by a Steering Group, comprising the Commissioner and Deputy Commissioners, which met regularly to make strategic decisions and provide oversight.

During 2018, leading up to the 25 May 2018, the Programme entered an 'Implementation Phase' which involved significant work to:

- Engage extensively, as a key stakeholder in the new regulatory regime under the GDPR and the Law Enforcement Directive, with the Department of Justice and Equality in relation to the drafting and preparation of the Data Protection Bill 2018 which was published in early 2018;
- Further enhance awareness by organisations across the public and private sectors in preparation for the application of the GDPR, as well as increasing information for members of the public to better understand their rights. This was achieved through a range of public awareness campaigns, including public media campaigns in addition to participation in a large number of speaking events;
- Further detail the organisation's future state internal procedures having regard to the Data Protection Bill 2018 (as it then was), the GDPR and Law Enforcement Directive, as well as the clarifications and guidance issued by the Article 29 Working Group. This was achieved through detailed analysis of the appropriate application of the new legislation, mapping the core 'future state' business processes, testing these using post-GDPR scenarios and benchmarking these procedures against other similar organisations;
- Grow the DPC team through recruiting new staff with a wide range of specialisms, including expertise in data protection, legal, technology, investigation and regulation. In the period 1 January to 24 May 2018, the DPC recruited 16 new staff and the DPC commenced the preparatory planning work for a major recruitment campaign, involving five Public Appointments Service competitions, which rolled out in the summer of 2018;
- Develop and provide intensive staff training to enhance the organisation's expertise and capability in the interpretation and application of data protection legislation, particularly the GDPR, Law Enforcement Directive and the new Data Protection Bill 2018;
- Prepare the office to act as the Lead Supervisory Authority (LSA) in certain cross-border cases in alignment with the EU 'consistency mechanism', often referred to as the One-Stop-Shop (OSS). This was achieved by continuing to engage with other Data Protection Authorities (DPAs), refining OSS procedures and training staff on the use of the system that supports OSS related communications between DPAs;
- Design and commence the build of a new website. This work included the review and update of the DPC's current website to provide updated GDPR information and implement new webforms pending the go-live of the new user-friendly DPC website. The new DPC website will provide comprehensive online web-forms which will enable requests, notifications, concerns and queries to be electronically submitted to the DPC thus facilitating more effective engagement between DPC, individuals and organisations;
- Design and build a new fit-for-purpose Case Management System (CMS) to enhance the timeliness and efficiency of how the DPC handles cases through to completion. A Case Management System was procured and the DPC's business and technical system requirements were specified in this period; and
- Support the decommissioning of processes that would no longer be required post the GDPR go-live date. This was achieved by identifying and ceasing such processes, including the removal of the registration process.

In addition, during the period from 1 January to 24 May 2018, work was undertaken to effect the transition to the new 'Data Protection Commission'. This has included activities to re-brand the office and scope the internal changes that will be required to prepare the office to become its own 'Accounting Officer'.

GDPR Awareness and Outreach

In the period leading up to 25 May 2018, the DPC launched a major initiative to raise awareness of the GDPR, 'Preparing Ireland for the GDPR' which identified and coordinated a number of communication streams aimed at raising awareness among a variety of sectors and the public in Ireland. National surveys carried out in May 2017 and again in May 2018, demonstrated a doubling of awareness of GDPR in the SME sector during this period. In May 2018, the result confirmed that over 90% of businesses were aware of the GDPR.

A number of the headline activities undertaken as a part of the awareness drive were as follows:

Public Information campaign

In the period 1 January to 24 May 2018, the DPC implemented a broad-based media campaign to raise public awareness of the change in law. This campaign included front-page newspaper adverts in the major daily newspapers, cinema adverts, radio adverts, and digital takeovers of online news outlets, which used content-only targeting to reach our audience. The campaign reached over 80% of Ireland's adult population.

Direct engagement

As part of the DPC's commitment to driving awareness of the GDPR, the office maintained an active outreach schedule during this period and engaged with a broad base of Irish and international stakeholders, including the media. The DPC contributed regularly to domestic and international media from 1 January to 24 May 2018, including the Wall Street Journal, the New York Times and the Financial Times.

The Commissioner and her staff spoke and presented at events on almost 120 occasions from 1 January 2018 to 24 May 2018, including conferences, seminars, and presentations to individual organisations from a broad range of sectors. Examples include:

National

- Association of Data Protection Officers — 10th Annual National Data Protection Conference 2018
- Zero Day Con — Cyber Security Conference
- Social Care Ireland Annual Conference 2018
- Adoption Authority Forum
- Public Sector Communications Group
- Data Sec 2018
- Sunday Business Post and iQuest: 2018 GDPR Summit
- RDS Economic Vision 2020 Business Breakfast
- Chartered Institute of Internal Auditors Ireland Annual Conference
- Health and Safety Review Annual Conference 2018

International

- International Association of Privacy Professionals (IAPP) Summit, Washington
- 8th EDPD Conference 2018, Berlin
- Conference of European Data Protection Authorities 2018, Albania

GDPRandYou.ie microsite

In 2017, the DPC created a microsite (www.GDPRandYou.ie) to serve as a central hub for all of its GDPR related resources. All of these resources are free to download. This website was promoted by the Irish government, industry representative bodies and other key stakeholders as an essential preparatory tool in advance of 25 May 2018.

Guidance documents available through www.GDPRandYou.ie included introductory material to the GDPR, an SME toolkit, a comprehensive guide to the rights of individuals, a guide for microenterprises and general guidance on key provisions of the GDPR such as DPO requirements, Data Protection Impact Assessments, the One-Stop-Shop provision and Controller-Processor contracts.

The DPC published a guidance document, 'Preparing your organisation for the GDPR — a guide for SMEs', at the end of 2017 and it was distributed and downloaded substantially up to 25 May 2018. This digital publication was made available free-of-charge in a downloadable PDF format on www.GDPRandYou.ie. The publication is a practical toolkit for small businesses that guides the systematic assessment of their data protection practices and preparedness for GDPR compliance. The checklist tool within the guide provides a walk-through guide on assessing current data protection practices against the requirements of the GDPR under a number of categories. The guide was designed in consultation with representatives from the SME sector, helping to ensure that the guide was of real value to SMEs.

The site also provided links to all of the Article 29 Working Party's GDPR guidance materials and the websites of all other EU data protection authorities.

Digital presence

The DPC has continued to promote GDPR awareness through its Twitter page, and in 2018 launched a LinkedIn page to bolster its social media presence. The DPC has used these platforms to disseminate guidance documents, promote awareness to both individuals and organisations through posters and infographics. The DPC Twitter account has a weekly organic reach in the tens of thousands, with an impression reach of over 170,000 in the week of 25 May 2018 alone.

GDPR Conference

In January 2018, the DPC hosted an international conference on 'Delivering Accountability under the GDPR'. This landmark, practical conference allowed almost 500 delegates from public sector organisations and SMEs to benefit from the experience and expertise of leading global privacy specialists, including senior representatives from the DPC, the Center for Information Policy Leadership, Apple, Facebook, MasterCard Worldwide, HP, Accenture, Google, and Arthur Cox, among others. Delegates benefitted from practical, hands-on workshops and exercises, and had the opportunity to shape the conversation by submitting questions through their phones directly onto the conference screen.

The DPC undertook this initiative in order to create a valuable learning event for those organisations that were most anxious about the introduction of the GDPR — SMEs and public sector organisations. The DPC is proud to have provided a unique event that allowed these organisations to gain expert, yet practical, training and insight from leading global experts.

Outcomes of awareness initiative

The DPC commissioned surveys in May 2017 and May 2018 to provide concrete metrics to measure the impact of the "Preparing Ireland for the GDPR" awareness initiative. The survey results show a remarkable two-fold increase in GDPR awareness amongst SME businesses in Ireland (90% in May 2018) compared to last year (44% in May 2017). In addition, in 2018 compared to 2017, five times more SME business executives demonstrated knowledge of the consequences of the GDPR for their organisations, along with a two-fold increase in pre-compliance activity in the small to medium enterprise sector.

Both our www.GDPRandYOU.ie guidance and our video adverts have been cited by the National Adult Literacy Agency of Ireland as exemplifying the principles of accessibility and understandability.

The DPC "Preparing Ireland for the GDPR" initiative made a very significant contribution to achieving an extraordinary level of GDPR awareness among Irish business and the public. Over 80% of the Irish public was reached by our campaign, leading to GDPR awareness of over 90% in the business community.

EU and International

The DPC continued to engage extensively with stakeholders outside of Ireland that would be subject to the GDPR or that were advising clients that would be subject to the GDPR. Engagements included the participation in January by the Commissioner in a detailed panel debate on international transfers of data alongside Bruno Gencarelli of the EU Commission at the popular CPDP conference in Brussels. In early March, the Commissioner and Deputy Commissioner John O'Dwyer travelled to San Francisco to give a number of talks on the GDPR to large audiences of data protection practitioners and technologists and engaged in detailed bilateral meetings with a number of companies around their preparations for the GDPR.

This was a very worthwhile trip as it allowed the DPC identify aspects of GDPR that were causing confusion. At the end of March, the Commissioner and Deputy Commissioner, John O'Dwyer, travelled to Washington DC to participate at the IAPP DC conference and in a series of side events and bilateral meetings in order to clarify the GDPR's principles alongside a number of other EU data protection authorities.

In April, the DPC took part in the IAPP London conference and was able to share practical details of how controllers could engage in notifying breaches under the mandatory GDPR requirement.

Article 29 Working Party

The DPC continued its active participation in the Article 29 Working Party (WP29) Plenary and subgroups, working closely with our EU and EEA counterparts. During this critical pre-GDPR period from 1 January to 24 May 2018, DPC staff contributed to the development of guidelines, working materials and draft operational procedures across all WP29 subgroups:

- Borders, Travel and Law Enforcement;
- Cooperation;
- eGovernment;
- Enforcement;
- Financial Matters;
- Fining Taskforce;
- Future of Privacy;
- International Transfers;
- IT Users;
- Key Provisions;
- Social Media; and
- Technology.

In addition, the DPC took a leadership role in the development of some key WP29 documents:

- Having acted as lead rapporteur for the WP29's development of Guidelines on Transparency that were published at the end of 2017, the DPC led the work on revising these guidelines in the early part of 2018, following EU-wide open consultation, with the final guidelines approved by WP29 in April 2018;
- The DPC acted as co-rapporteur on the WP29 Guidelines on Accreditation which were approved and published for open consultation in February 2018, and on the related Guidelines on Certification, whose approval and publication followed in July 2018;
- The DPC continued its lead rapporteur role in the drafting of Guidelines for Codes of Conduct, to assist data controllers in demonstrating their compliance via this important accountability tool, with these guidelines due to be approved and published for open consultation by the end of 2018;

- As lead rapporteur, the DPC commenced work on a paper on the contractual necessity basis under Article 6(1)(b) GDPR for processing personal data, in the context of the provision of online services, with this work continuing; and
- In May 2018, the DPC was appointed co-coordinator of the newly-formed Social Media subgroup whose role is to develop guidance and set strategic priorities relating to the processing of personal data by social media companies.

The Article 29 Working Party (WP29) ceased to exist on 25 May 2018 and was replaced by the European Data Protection Board (EDPB). The membership of both bodies is the same, consisting of the data protection supervisory authorities of each EU and EEA member state as well as the European Data Protection Supervisor. However, the functions of the EDPB are significantly augmented from those of the WP29, including oversight of the consistent application of the GDPR and ensuring collaboration amongst EU data protection authorities under the Co-operation and Consistency mechanisms in the GDPR.

During the period from 1 January to 24 May 2018, the DPC was particularly active in WP29's preparations for this fundamental change, in terms of cooperation procedures, operational protocols and information sharing tools. These preparations were of particular importance to the DPC, given the presence in Ireland of so many multinationals, including technology and social media companies. Under the One-Stop-Shop model, the DPC is the lead supervisory authority with oversight of the cross-border processing of personal data by these companies.

Registration

Registration of Data Controllers and Processors under the Data Protection Acts 1988 and 2003 for the period 1 January to 24 May 2018; and

Establishment of a notification system for Data Protection Officers under the GDPR from 25 May 2018.

Under the Data Protection Acts 1988 and 2003, certain categories of data controllers and processors were legally bound to register with the DPC on an annual basis. This legal requirement for registration came to an end on 25 May 2018 with the application of the GDPR and enactment of the Data Protection Act 2018.

During the period 1 January to 24 May 2018, the DPC's two core activities in the area of registration were as follows:

a) to implement the registration system provided under the Data Protection Acts 1988 and 2003, in respect of those organisations obliged to register up to 25 May; and

b) to create awareness regarding the new requirement applicable under the GDPR for relevant organisations to notify the DPC of its 'Data Protection Officer' (DPO) and to bring to the attention of data controllers and processors of the cessation of the registration requirement under the Data Protection Acts from 25 May onwards.

a) Continued operation of the Data Protection Acts 1988 and 2003 registration system

Until 25 May 2018, certain categories of data controllers and data processors were required to register with the office of the Data Protection Commissioner.

Section 16(1) of the Data Protection Acts 1988 and 2003 defined the persons to whom the registration requirement applied. The requirement to register applied to all data controllers and data processors processing personal data on behalf of such data controllers unless:

- the data controller was a 'not-for-profit' organisation;
- the processing of personal data was for the purpose of a publicly available register;
- the processing was of manual data (except for any specific categories of prescribed data); or
- exemptions under Regulation 3 of SI 657 of 2007 applied.

During the period 1 January to 24 May 2018, the total number of register entries was 6,885, comprised as follows:

Category of registrants	No. of Registrants
Financial and credit institutions	449
Insurance organisations	274
Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts	49
Telecommunications/internet providers	36
Health sector	2,174
Pharmacists	1,103
Miscellaneous	1,230
Data processors	1,570

Registration entries for the years 2015 to 2018 are as follows:

Year of Registration	Total No. of Registrations
2015	6,235
2016	6,901
2017	7,143
2018	6,885

The last date on which registration applications and fees were accepted was 17 May 2018, and the public register was updated for the final time on 18 May 2018.

b) Establishment of a new notification system from 25 May 2018 for Data Protection Officers under the GDPR

The GDPR created a new obligation under Article 37 whereby certain organisations are required to appoint a designated Data Protection Officer (DPO). Organisations are also required to publish the contact details of their DPO and provide these details to their lead supervisory authority. The purpose of this requirement is to ensure that individuals (internal and external to the organisation) and the data protection authority can easily and directly contact the DPO without having to contact another part of the organisation.

Under the GDPR an organisation is required to appoint a Data Protection Officer where:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their 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 also provides for regulations to be made specifying further situations in which the designation of a DPO may be required.

A DPO may be a member of staff at the appropriate level with the appropriate training, an external DPO, or one shared by a group of organisations, which are all options provided for in the GDPR.

During the period 1 January to 24 May 2018, the DPC established new procedures and information systems in order to receive notifications from relevant organisations of the designation of a DPO from 25 May 2018 onwards.

The DPC has implemented a webform on its website for the notification of DPOs by organisations. There is no fee applicable for this process.

Corporate Affairs

Overview

The Corporate Affairs unit of the DPC is responsible for the implementation and development of measures to ensure organisational compliance with corporate governance requirements and compliance with legislation. The unit is also responsible for supporting the organisation's operational and strategic objectives by ensuring that administrative, financial, HR and ICT services are in place.

Finance

The funding of the DPC by Government has increased significantly in recent years from €1.7 million in 2013 to an allocation of €11.6 million in 2018 (comprising €7.3 million pay and €4.3 million non-pay allocation). The DPC acknowledges the significant increase in funding in recent years and welcomes the Government's continuing commitment to meeting the resourcing needs of the organisation in performing its expanding role as one of the leading data protection authorities in the EU.

The DPC also collected revenue for the statutory registrations of data controllers and processers in the period between 1 January and 24 May 2018. As referred to in the Registration section of this Report, under the Data Protection Acts 1988 and 2003, certain categories of data controllers and data processors were required to register with the office of the Data Protection Commissioner. However, with the implementation of the GDPR and the new Data Protection Act on 25 May 2018, the legal requirement for registration came to an end and from that date the DPC no longer collects this revenue.

Details of statutory registration payments received by the DPC between 1 January and 24 May 2018 will be made available in the Annual Financial Statement of the office of the Data Protection Commissioner in respect of that time period.

The Department of Justice and Equality channels the DPC's budget through its vote under subhead A.7 which is part of 'Programme A- Leadership in and oversight of Justice and Equality policy and delivery'. 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 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 (FSS), its central accounting system. The DPC's payroll and expense payments are processed by the Payroll Shared Service Centre (PSSC) which is under the Department of Public Expenditure and Reform's (DPER) remit.

Annual Financial Statement in respect of the office of the Data Protection Commissioner covering the period from 1 January to 24 May 2018

The Annual Financial Statement in respect of the office of the Data Protection Commissioner covering the period from 1 January to 24 May 2018, is in preparation for submission to the Comptroller and Auditor General (C&AG) for audit. Once the audit is concluded and the Annual Financial Statement has been approved by the Comptroller and Auditor General, it will be appended to this Report.

Staff Resources

Up to 24 May 2018, the Commissioner, independent in the performance of her functions, was appointed by Government, in accordance with the Data Protection Acts 1988 and 2003. As of 25 May 2018, the Data Protection Commission is established in accordance with the provisions of the Data Protection Act 2018 and in accordance with the GDPR and is independent in the performance of its tasks and exercise of its powers.

As at 24 May 2018, the office of the Data Protection Commissioner had a staff of approximately 100, across its Dublin and Portarlington locations, to support the implementation of these functions.

One of the key priorities of the DPC during the period covered by this Report was to continue to expand and develop the staff team at the DPC. In the period 1 January to 24 May 2018, the DPC recruited 16 new staff and commenced planning a major recruitment campaign, involving five Public Appointments Service competitions, which rolled out in the summer of 2018. As part of these campaigns the DPC is recruiting new staff with a wide range of specialisms, including expertise in data protection, legal, technology, investigation and regulation.

Furthermore, staff training and continuous development is a key priority for the DPC. During the period of this Report, the DPC developed and provided intensive staff training to enhance the organisation's expertise and capability in the interpretation and application of data protection legislation, particularly the GDPR, Law Enforcement Directive and the new Data Protection Act 2018.

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

While the Data Protection Commissioner is an independent body, the organisation ensures the oversight of its administration follows the requirements set out in the Code of Practice for the Governance of State Bodies, 2016.

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 which underpin the relationship between the office and the Department of Justice and Equality. As the DPC is independent in the performance of its functions under the provisions of the Data Protection Acts 1988 and 2003, and under the GDPR and Data Protection Act 2018 (with effect from 25 May 2018), it is not subject to a Performance Delivery Agreement with the Department of Justice and Equality.

The DPC's Statement of Internal Controls, prepared in accordance with the Code of Practice, provided at Appendix V.

Statutory Governance Requirements

While the DPC is an independent body, we ensure that oversight of our administration follows the requirements set out for all public sector bodies in the Code of Practice for the Governance of State Bodies, 2016. All expenditure is accounted for to the Exchequer, and the DPC is audited annually by the Comptroller and Auditor General. Daily interactions with citizens, businesses and other key stakeholders provides additional oversight of the work we undertake. Appeals of the Commissioner's statutory decisions can be made to the Courts.

The DPC is cognisant of its public sector duty under the Irish Human Rights and Equality Act 2014.

Strategic Planning

During the period covered by this Report, the office of the Data Protection Commissioner operated in accordance with the provisions of the Data Protection Acts 1988 and 2003. It also carried out its functions in line with the key strategic goals as set out in its Statement of Strategy for 2017-2018. The delivery of the organisation's remit was underpinned by unit business plans and the goals of individual staff members. The organisation's progress in implementing the 2018 priority actions was monitored on an ongoing basis by the SMC.

With the implementation of GDPR and new data protection legislation, the DPC plans in 2018 to undertake the development of a Regulatory Strategy. This Strategy will provide the foundation for the DPC's approach in the performance of its regulatory functions and will underpin the development of a new Statement of Strategy.

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 implemented the procedures outlined in its Risk Management Policy and maintained a Risk Register in line with Department of Finance guidelines. This included carrying out an appropriate assessment of the DPC's principal risks, including a description of the risk and associated measures or strategies to control and mitigate these risks. The Risk Register is compiled by Corporate Affairs 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 prepared to take on new and enhanced supervisory functions and responsibilities set out by the GDPR;
- building organisational capacity including further developing the expertise of the DPC's staff as well as the 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; and
- 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 a 'Scheduled Office' with its own Vote and 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 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.

DJE Internal Audit Unit assist the DPC by providing reasonable audit assurance that significant operating risks are identified, managed and controlled effectively. DJE Internal Audit Unit undertook an audit of the DPC's financial controls in early 2018, with the report brought before the SMC and the DJE Audit Committee. The audit did not identify any significant issues.

Freedom of information

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

From 1 January to 24 May 2018, this office received a total of 12 requests under the FOI Act. Of the 12 requests received in the period 1 January to 24 May 2018, seven were deemed to be out of scope, and no cases were appealed to the Office of the Information Commissioner.

The DPC dealt with one request in 2018 under the European Communities (Access to Information on the Environment) Regulations 2007, S.I. 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.

Request by type	Category total	Outcome
Administrative Issues	5	2 Granted
1 Part Grant		
1 Dealt with outside of FOI		
1 Withdrawn		
Personal data (outside of scope)	1	1 Refused
Matters outside the scope of the Acts	6	6 Refused
Live cases	Nil	

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. This office will continue to provide Irish language service as per our Customer Charter and Irish language information via our website.

Appendix I
List of Organisations Audited or Inspected (between 1 January and 24 May 2018)

The Commissioner would like to thank all of the organisations audited and inspected between 1 January and 24 May 2018 for their cooperation. The inspection teams found there was a reasonably high level of awareness and compliance with, data protection principles in the majority of organisations audited. At the same time, many organisations required remedial action in certain areas. The inspection teams noted the efforts made by data controllers and processors to put procedures in place to ensure that they are meeting their data protection responsibilities in full.

- Sherry Fitzgerald Lettings
- Dublin City Council
- Vodafone
- Private Security Authority
- Dublin Property Rentals
- Terrie Dunne Lettings
- Galway City Council
- NetDrNow, Swords (visual inspection)
- D15GP, Blanchardstown (visual inspection)
- St. Corban's Boys National School
- Adamstown Community College
- Fingal County Council
- Halfords
- Cork City Council
- Minnock Agri Enterprises
- FRS Training
- Bank of Ireland
- Hostelworld
- Drumcondra Credit Union
- Limerick City and Co Council

SIU Inspections (Special Investigations Unit)

- Dowling and Company, Leixlip, Co. Kildare
- Blackrock Garda Station, Blackrock, Co. Dublin
- Private Investigation, Celbridge, Co. Kildare

Appendix II
Case Studies

CASE STUDY 1: Prosecution of Guerin Media Limited

The DPC received unrelated complaints from three individuals about unsolicited marketing emails that they had received from Guerin Media Limited. In all cases, the complainants received the marketing emails to their work email addresses. None of the complainants had any previous business relationship with Guerin Media Limited. The marketing emails did not provide the recipients with an unsubscribe function or any other means to opt out of receiving such communications. Some of the complainants replied to the sender requesting that their email address be removed from the company's marketing list. However, these requests were not actioned and the company continued to send the individuals further marketing emails. In one case, nine marketing emails were sent to an individual's work email address after he had sent an email request to Guerin Media Limited to remove his email address from its mailing list.

The DPC's investigation into these complaints established that Guerin Media Limited did not have the consent of any of the complainants to send them unsolicited marketing emails and that it had failed in all cases to include an opt-out mechanism in its marketing emails.

The DPC had previously received four similar complaints against Guerin Media Limited during 2013 and 2014 in which the company had also sent unsolicited marketing emails without having the consent of the recipients to receive such communications and where the emails in question did not contain an opt-out mechanism. On foot of the DPC's investigations at that time, the DPC warned Guerin Media Limited that it would likely face prosecution by the DPC if there was a recurrence of such breaches of the E-Privacy Regulations. Taking account of the previous warning and the DPC's findings in its current investigation, the DPC decided to prosecute Guerin Media Limited for 42 separate breaches of the E-Privacy Regulations.

The prosecutions came before Naas District Court on 5 February 2018 and the company pleaded guilty to four sample charges out of the total of 42 charges. Three of the sample charges related to breaches of Regulation 13(1) of the E-Privacy Regulations for sending unsolicited marketing emails to individuals without their consent. The fourth sample charge related to a breach of Regulation 13(12)(c) of the E-Privacy Regulations for failure to include an opt-out mechanism in the marketing emails. The Court convicted Guerin Media Limited on all four charges and imposed four fines each of €1,000, i.e. a total of €4,000.

The company was given a period of six months in which to pay the fine. It also agreed to make a contribution towards the prosecution costs incurred by the DPC.

Marketing to work email addresses

There is a common misconception that the sending of email communications to individuals at a work email address is a form of business-to-business communication where consent of the individual is not required. The E-Privacy Regulations allow a carve out to the default rule (i.e. that the sending organisation must have the consent of the receiving individual) which allows for such communications to be sent to an email address that reasonably appears to be one used by a person in the context of their commercial or official activity. However, in order to rely on this exception to the general rule requiring consent, the sender must be able to show that the email sent related solely to the recipient's commercial or official activity, in other words, that it was a genuine business-to-business communication. In effect, this means that marketing material that is directly relevant to the role of the recipient in the context of their commercial or official activity (i.e. within their workplace) may be sent by an organisation without the prior consent of the recipient. However, this was not the case in the circumstances at issue. Instead, the marketing communications sent by Guerin Media Limited related to attempts by that company to sell advertisement space in various publications and to sell stands at exhibitions. However, none of the individual complainants who received those communications had any role in relation to marketing related matters within their own workplaces.

While not directly applicable here, as the complainants were all individuals, organisations should also take note of a further rule in the E-Privacy Regulations concerning situations where the recipient of an unsolicited direct marketing communication is not an individual (e.g. the email address used is a solely company/corporate one and does not relate to the email account of an individual, whether at work or otherwise). In such a case where the company/ corporate recipient notifies the sender that it does not consent to receiving such emails, it is unlawful for the sender to subsequently send such emails.

This case is an important demonstration that any organisation engaging in electronic direct marketing activities should carefully establish the basis on which it considers that the primary default rule requiring a sending organisation to have the consent of the recipient does not apply to it in any given case, and how it can demonstrate

this. The case also illustrates the importance of including an opt-out mechanism in each and every electronic direct marketing communication as failure to do so constitutes a separate offence, (in addition to any offences in relation to failure to obtain consent) in respect of each such email/ message.

CASE STUDY 2: Prosecution of AA Ireland Limited

In December 2017 the DPC received a complaint from an individual who had received unsolicited marketing text messages from AA Ireland Limited. He informed the DPC that he had recently received his motor insurance renewal quotation from his current insurance provider and had decided to shop around to try to get a more competitive quotation. One of the companies he telephoned for a quotation was AA Ireland Limited. The complainant informed the DPC that he had expressly stated to the agent who answered his call that he wanted an assurance his details would not be used for marketing purposes and that he had been given that assurance by the agent. The phone call continued with the agent providing a quotation. The complainant noted that the quotation was higher than the renewal quotation from his current insurance provider and the complainant had indicated to the agent that he would not be proceeding with the quotation offered by AA Ireland Limited. The complainant informed the DPC that at his point in the call he had reiterated to the agent that he should not receive marketing material and he was once again assured by the agent that this would not happen.

The essence of the complainant's complaint however was that the day after the phone call in question he had received a marketing text message from AA Ireland Limited offering him €50 off the quote provided. A further similar text message was sent to his mobile phone one day later. The complainant stated in his complaint that he felt that this action was a blatant breach of his very clear and precise instructions that he did not wish to receive any marketing communications.

During the course of our investigation, AA Ireland Limited confirmed that it had sent both text messages to the complainant and admitted that it had not obtained consent to send these messages to the complainant. The company acknowledged that the complainant had requested that he not receive marketing messages, that the complainant's request should have been actioned and that his details should not have been used for marketing purposes. The company claimed that the incident arose as a result of human error. It explained that the correct process had not been followed by the agent so that the complainant's details had been recorded with an opt-in for him to receive marketing messages therefore resulting in marketing text messages being sent to him.

As the DPC had previously issued a warning in separate circumstances to AA Ireland Limited in relation to unsolicited marketing communications, in this instance the DPC decided to initiate prosecute proceedings. At Dublin Metropolitan District Court on 14 May 2018 AA Ireland Limited entered a guilty plea to one offence. It also agreed to cover the prosecution costs incurred by the DPC. In lieu of a conviction and fine, the Court applied Section 1(1) of the Probation of Offenders Act.

CASE STUDY 3: The Dublin Mint Office Limited

The DPC received a complaint on 13 October 2017 from an individual who had received two marketing telephone calls that same day, one targeted at him and one at his son, from The Dublin Mint Office Limited. The caller in each case had attempted to sell commemorative coins. In his complaint, the complainant explained that he had registered online a few months earlier with the company for an online offer on his own behalf and on behalf of his son, providing the same telephone contact number for both of them during the online registration process. The complainant stated that he ticked the marketing opt-out box during that online registration process.

During the course of the DPC's investigation, The Dublin Mint Office Limited admitted that it had made the marketing telephone calls. It explained that when the complainant supplied his telephone number during the online application process in May 2017 the order form had only offered an opt-in option to receive marketing mails and emails. The company confirmed that the complainant had not selected the opt-in option and he was therefore marked as opt-out for marketing mails and emails only. The company explained that a gap in the system in place at the time only allowed for an opt-in to marketing mails and emails but that it was not an opt-out for telesales. As a result, the complainant's details were included in a list for a follow-up telesales call. The company informed the DPC that it had written to the complainant to apologise for the inconvenience caused to him and to his son by its inadvertent mistake.

The DPC had previously issued a warning to The Dublin Mint Office Limited in September 2017 concerning other complaints which had been made to the DPC concerning unsolicited marketing communications by the company. The DPC therefore decided to prosecute The Dublin Mint Office Limited. At Dublin Metropolitan District Court on 14 May 2018 the company pleaded guilty to two charges in relation to both marketing telephone calls. It also agreed to cover the DPC's prosecution costs. In lieu of a conviction and fine, the Court applied Section 1(1) of the Probation of Offenders Act.

CASE STUDY 4: Access Request made to NAMA

Background

In February 2018, the DPC issued a decision on a complaint which had been made to it by two individuals against the National Asset Management Agency (NAMA). The complaint concerned allegations of non-compliance with a joint access request which had been made to NAMA in September 2014 by the complainants who were the directors and/or shareholders of a number of companies whose loans had transferred to NAMA. Certain personal loans of those individuals had also transferred to NAMA. The joint access request which had been made to NAMA expressly referenced personal data held by NAMA in connection with both the personal loans and the company loans.

NAMA responded to the complainants in October 2014, asking them to identify which of a number of categories of personal data (which NAMA itself had identified) that they wished to receive. The complainants replied, objecting to the manner in which NAMA's response had sought to limit the scope of the request. NAMA subsequently provided the complainants with a copy of the personal data which it considered the complainants were entitled to but noted that it was not required to provide personal data which was subject to legal privilege, which comprised confidential expressions of opinion or which would prejudice the interests of NAMA in respect of a claim or which would prejudice the ability of NAMA to recover monies owed to the State. However, NAMA did not identify the personal data in respect of which it considered such exemptions from the right of access applied. While the personal data provided by NAMA to the complainants related to the personal loans of the complainants which had previously transferred to NAMA, it did not include personal data relating to the complainants as directors and/or shareholders in the companies whose loans had transferred to NAMA.

Complaint to the DPC

The data subjects subsequently made a complaint to the DPC which alleged:

- that NAMA had failed to provide all of the complainants' personal data to them;
- that NAMA had incorrectly applied exemptions under the Data Protection Acts 1988 and 2003; and
- that even if NAMA was entitled to rely on one or more exemptions, that it was obliged to provide the complainants with a description of the personal data so that they had a reasonable and fair opportunity to consider whether it did fall under an exemption; and
- that NAMA had failed to conduct searches for personal data relating to ten additional categories of information identified by the complainants.

NAMA's position on the complaint

NAMA stated that it had fully complied with the access request. Following an exchange of correspondence with the DPC, NAMA contended:

- that "corporate data", i.e. information relating to the loans of the companies linked to the complainants did not fall within the definition of "personal data";
- that it was released from its obligations to provide access to personal data contained within the totality of the records held in relation to both the personal loans and the company loans, on the basis that conducting such searches would require 'disproportionate effort' on the part of NAMA to do so; and
- that it was appropriate for NAMA to rely on statutory exemptions to the right of access, as provided under Sections 5(1)(a), 5(1)(f) and 5(1)(g) of the Data Protection Acts 1988 and 2003.

DPC Investigation

In a submission to the DPC, NAMA provided estimates of the number of relevant records it held, and the potential financial cost of completing a comprehensive search for all personal data requested. NAMA confirmed that it had not conducted searches for the complainants' personal data held in relation to company loans.

In order to substantiate its position, NAMA agreed to conduct sample searches for personal data in respect of a particular two-month period. Authorised officers on behalf of the DPC conducted three on-site investigations at NAMA premises to corroborate NAMA's position on issues relating to its searches. Following a review of the sample searches carried out, DPC officers were not satisfied that a comprehensive search would involve a disproportionate effort on the part of NAMA, or that information held by NAMA relating to the complainants' company loans did not also contain personal data of the complainants.

Following engagement between the DPC and NAMA, additional personal data was released to the complainants. However, efforts to resolve this matter informally were to no avail. The DPC subsequently issued a lengthy statutory decision running to some 67 pages in relation to the complaint. This decision addressed the three core issues referred to above. The DPC's findings on each of these issues was as follows.

The Commissioner's Decision

(1) The Corporate Data Issue

While NAMA acknowledged that the complainants' names appeared in records relating to the company loans, reflecting that they were directors and/or shareholders of the companies in question and while NAMA accepted that the complainants' names were their personal data, it contended that this did not make the other information in those records their personal data. The complainants' position meanwhile was that there was no doubt but that information relating to a person in their capacity as a company director could constitute personal data. They also pointed to the fact that information referencing an assessment of their performance / conduct or the evaluation of their assets constituted personal data even it if was concerned with company loans or the business of those companies. The complainants also contended that while records in relation to the company loans and their personal loans were held separately, the reality was that all of NAMA's dealings with them were interconnected.

The DPC in her decision noted that the mere fact of one of the complainant's names appearing in records relating to the company loans (for example if they had simply signed a commercial agreement in their capacity as director of a company) was not sufficient in and of itself for other information in that agreement to constitute personal data. However, the records which had been identified through the sample searches bore out the complainants' contentions that those records could not be assumed to contain no personal data at all. The DPC noted by way of example that it was clear from a document, the title of which referred to a NAMA board meeting, that while the board meeting had discussed and considered a business plan referable to one of the companies, there was information in that document relating to the financial assets of the complainants in their personal capacities. The DPC accepted the complainants' position that the records held by NAMA regarding the company loans contained at least some personal data relating to them. Therefore the DPC considered that NAMA must at the very least, identify the records or types of records in which the complaints were identified by name or otherwise but which NAMA considered did not constitute personal data, and provide sufficient information for the complainants to understand why it was said that those records or types of records do not constitute or contain personal data.

(2) The Disproportionate Effort Issue

The DPC then considered whether the time and money costs involved in NAMA conducting searches of the records held in relation to the company loans would be disproportionate relative to the amount of personal data that might be found and disclosed to the complainants. The DPC noted that while there is no express obligation on a data controller to search for personal data in order to comply with a properly made access request, she accepted that there was an implied obligation on a data controller to undertake searches so as to identify what personal data it might hold on a requester. The question for consideration concerned the nature and extent of this implied duty. The DPC noted that the disproportionate effort obligation found in Section 4(9)(a) of the Data Protection Acts 1988 and 2003, on the face of that provision, applied only to limit the obligation to provide to the data constituting the personal day in permanent form. However, it did not limit the earlier steps in the process such as the obligation to search for the data. While the DPC referred to jurisprudence from the UK Courts which has established that the implied obligation to search for personal data is limited to a reasonable and proportionate search, she noted that she was not aware of any judicial authority in Ireland dealing with the nature or extent of a controller's obligations to conduct searches in order to comply with Section 4 of the Data Protection Acts 1988 and 2003. While accepting that there was no obligation on her to recognise the principles established by the UK authorities, the DPC noted that one particularly pertinent decision to this effect (Deer v. University of Oxford) had previously been referenced by the Irish High Court (in the judgment of Coffey J. delivered on 26 February 2018 in the case of Nowak v. Data Protection Commissioner). The DPC considered that decision to be helpful in interpreting Sections 4(1) and 4(9) of the Data Protection Acts 1988 and 2003, particularly given its analysis of case law from the CJEU. On that basis the DPC therefore accepted NAMA's contention that the obligation to search for personal data was not without limits but rather NAMA was required to undertake reasonable and proportionate searches to identify the personal data of the complainants which it held.

The DPC then went on to consider whether NAMA had discharged this obligation, by carrying out the type of balancing exercise which had been contemplated in the UK case law, between upholding the data subject's right of access and the burden which it would impose on the data controller. In doing so, the DPC considered a number of factors bearing upon this balancing exercise, including the intrinsic significance of the personal data and its relative importance to the requesters. In this regard, the DPC noted that the personal data in question related to the business and financial interests of the complainants both personally and in respect of the companies of which they were directors and/ or shareholders. It was also considered relevant that (as evident from the correspondence seen by the DPC's officers) that the complainants were trying to bring about a situation in which the company loans would be dealt with by NAMA in a way that would ensure the survival of the companies and preserve the complainants' ability to retain some level of ownership or control in those companies. Consequently, the DPC considered the personal data held by NAMA to be of significant importance to the complainants.

The DPC then considered the countervailing points made by NAMA, including specific estimates (calculated on the basis of the results from the sample searches) provided to the DPC relating to the estimated number of hits produced if searches were to be carried out (approximately 62,000), the estimated number of relevant

records which would be identified following a review of those hits (approximately 12,600) and the estimated time which it would take to review, assemble and redact the material for release to the complainants (over 2,700 hours). It was also noted by the DPC that while NAMA had referred to the potential for technical solutions to counteract the manual input required, that NAMA had stated it was not something which it had assessed and its view was that should such solutions exist, they would incur a disproportionate cost of implementation.

The DPC found NAMA's estimates as regards the time and effort involved in carrying out the full period searched to be speculative in nature and lacking in specific detail, and that it had failed to discharge the burden of proof on it in this regard. This was particularly so in light of the fact that NAMA's previous position (prior to the sample searches having been conducted) that there was no personal data of the complainants held in the records relating to the company loans, had not been borne out in fact by reference to the results of those sample searches. NAMA had, it was noted, originally agreed to conduct searches for the whole period during which it held the company loans if the sample searches had demonstrated that there was personal data of the complainants held in the records relating to the company loans. However, some 14 months later NAMA had changed its position and decided not to undertake any further searches at all despite the sample searches having shown the presence of personal data in the company loans records. The DPC also considered that NAMA's claims (in the absence of an assessment to this effect) that (1) a technical solution would not be feasible and (2) its unparticularised claim that the disproportionate effort involved in carrying out the searches and providing the personal data identified would divert its resources away from its statutory remit, did not discharge the burden of proof to which it was subject in respect of its claims of disproportionate effort.

The DPC found that in refusing to conduct the searches NAMA had not sought to balance its rights against the complainants' rights but had set them at nought. NAMA had not discharged its obligation by conducting reasonable and proportionate searches to find relevant personal data and supply it. The DPC was not satisfied on the basis of the arguments and evidence put forward by NAMA that by conducting the searches this would constitute disproportionate effort on its part.

(3) The Statutory Exemptions Issue

The sample searches which had been carried out by NAMA led to the identification of 14 hard copy documents containing the personal data of the complainants, drawn from NAMA's records relating to both the company loans and the personal loans. However, NAMA withheld or redacted 3 of these documents on the basis of certain exemptions to the right of access. These exemptions related to Section 5(1)(g), Section 5(1)(f) and Section 5(1)(a) of the Data Protection Acts 1988 and 2003. As a preliminary matter the DPC found that NAMA must prove convincingly, and by evidence, meeting the civil standard of proof that each of the exemptions on which it sought to rely on did in fact apply in this case and operated to trump the complainants' rights of access.

In the case of the legal privilege exemption which NAMA claimed applied to an internal email passing between solicitors employed at NAMA, the DPC noted that this document on its face was labelled as attracting litigation privilege. However given that no litigation was in being between the complainants and NAMA at the time of its creation (and in fact the only litigation now in being had only come into existence some 2 to 3 years later), the DPC was not satisfied that NAMA had discharged the burden of proof on it to show that litigation privilege applied to the personal data in question. However, the DPC then went on to consider whether legal advice privilege applied and concluded that it did because the content of the email in question set out the basis on which certain issues relating to the personal loans might be considered and addressed. The DPC was therefore satisfied that the email in question was privileged and exempt from release under Section 5(1)(g) of the Data Protection Acts 1988 and 2003.

With regard to two further documents, NAMA claimed that the exemption in Section 5(1)(a) applied. This provides that the right of access does not apply to personal data kept for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or health board in any case in which granting access to the personal data would prejudice any such matters.The DPC applied the test for application of this exemption which had been set out in the UK judgment of Guriev & another v. Community Safety Development (UK) Limited [2016] EWHC 643. That case had concerned the equivalent exemption under the UK Data Protection Act 1998. The DPC found that NAMA had simply asserted that in the case of the two records in question, providing access to the personal data would have the effect of disclosing its strategy in dealing with liabilities. However NAMA had made no effort to explain the nature and effect of the prejudice that would be suffered if the personal data in question was released, how the release of it would lead to the prejudice, nor how applying the exemption was a necessary and proportionate interference with the complainants' rights having regard to the gravity of the threat to the public interest. In light of this lack of evidence, the DPC decided that it was not open to NAMA to rely on this exemption.

The final exemption relied on by NAMA and considered by the DPC was Section 5(1)(f) which provides that the right of access does not apply to personal data consisting of an estimate or kept for the purposes of estimating the amount of liability of a data controller on foot of a claim in respect of damages or compensation where granting access would be likely to prejudice the interests of the data controller in relation to the claim. The DPC found that no evidence had been put forward by NAMA as to the factual basis for relying on the exemption. For example, NAMA had not identified the prejudice which it would suffer if it provided the personal data, or how or

in what context the prejudice would arise. As NAMA had failed to discharge the burden of proof on it in relation to its claim to this exemption, the DPC found that it was not open to NAMA to rely on it.

Decision

Arising from the DPC's findings, the DPC concluded that NAMA was in breach of its obligations under Section 4(1)(a) and Section 4(9) of the Data Protection Acts 1988 and 2003.

CASE STUDY 5: Disclosure of CCTV footage from a direct provision centre

We received a complaint from solicitors for a resident of a direct provision accommodation centre in relation to an alleged disclosure of CCTV footage capturing the complainant's images. The accommodation centre in question is owned by the State (with responsibility for it resting with the Reception and Integration Agency (RIA) which sits within the Department of Justice and Equality). The centre is managed on a day-to-day basis by Aramark Ireland (Aramark). The alleged disclosure of the complainant's personal data came to her attention during her participation in a radio programme. The subject matter of that radio show concerned a matter that had arisen between residents of the accommodation centre and its staff. During the course of the radio programme, the radio host claimed that he had a copy of CCTV footage, which was apparently taken from a room in the accommodation centre, which allegedly showed an altercation between the complainant and another resident of the direct provision centre.

The complainant subsequently made complaints to RIA, to Aramark and to the radio station which had aired the radio programme in question. An access request for a description of all recipients to whom the complainant's personal data had been disclosed was also made on behalf of the complainant under Section 4 of the Data Protection Acts 1988 and 2003 to RIA. However, the complaint noted that RIA had not responded to that access request.

We commenced an investigation into the complaint seeking information from both Aramark and the RIA. The RIA informed us that it was liaising with Aramark and had requested a report from it. During the investigation, we established that Aramark was a data processor processing personal data on behalf of the RIA. Aramark submitted that CCTV is used for security purposes and to monitor health and safety within the accommodation centre. Aramark informed us that it processes personal data in line with the RIA's instructions and that access to the storage medium within the accommodation centre was limited to specific authorised personnel, with accompanying user name and passwords requirements.

In relation to the specific allegation of disclosure of the CCTV footage, Aramark told us that CCTV footage of an altercation involving the complainant had been downloaded by authorised personnel from Aramark and transmitted to the RIA. The reason for the download and transmission were that the captured events related to security, and health and safety issues. According to Aramark, due to the size of the file in question, the employee had saved the footage to a Google link for onward transmission to the RIA.

Aramark informed us about a detailed forensic IT enquiry that had been conducted in relation to the complaint, across its IT systems to identify whether any other disclosure of the CCTV footage had taken place. It maintained on the basis of its own investigations that the link had not been sent from any Aramark email account to an outside party other than the RIA. Amongst other things, as part of the forensic enquiry, Aramark said that it had checked internet logs on the Aramark computer used at the accommodation centre, searched the mailboxes of Aramark staff who worked at the accommodation centre and searched for email correspondence inbound and outbound relating to the incident. A data recovery program had also been installed on the computer in question to review all deleted content on the computer. No activity indicating disclosure of the CCTV footage to any third party had been identified. Aramark further informed us that the Google link no longer existed and was therefore not accessible.

Aramark also maintained that the authorised personnel who had downloaded the footage had confirmed that the footage had not been disclosed to any third party and that it had been deleted following transmission to the RIA.

Separately the RIA confirmed to us during our investigation that the Google link to the CCTV footage which it had received, referenced the complainant and another resident. It stated that a copy of the footage had not been retained by the RIA.

In relation to the management of the CCTV system in the accommodation centre, the RIA furnished us with certain documentation including Aramark's data protection and CCTV policies and a confidentiality agreement in place with Aramark. However, the RIA acknowledged during our investigation that there were no policies or practice documents in place for the management of CCTV operating in accommodation centres.

Ultimately neither Aramark nor the RIA were able to definitively confirm that CCTV footage in question had not been disclosed to the radio station. In relation to its non-compliance with the access request, the RIA's position was that it was waiting on a detailed report from Aramark and that it could not respond to the access request until it had received that report.

In her decision, the DPC found that the RIA did not respond to the request by the complainant for a description under Section 4 of the Data Protection Acts 1988 and 2003 of all recipients to whom the personal data was disclosed, within the prescribed timeframe of 40 days. This was in direct contravention of RIA's obligation under that provision.

In relation to the oversight of the processing carried out by Aramark as a processor for RIA, based on the submissions made by both the RIA and Aramark in the course of the DPC's investigation, there was no evidence of a written contract in place which delineated the respective obligations applicable to the RIA and Aramark in relation to the processing of personal data by Aramark on the RIA's behalf. This constituted a contravention by the RIA, as the data controller, of Section 2C(3) of the Data Protection Acts 1988 and 2003.

Although the DPC was unable to establish how the CCTV footage in question came to be in possession of a radio station, the DPC found that ultimately the complainant's rights were infringed. In this regard both the RIA and Aramark failed in their duty of care to the complainant by failing to ensure that appropriate security measures were taken against the unauthorised disclosure as required by Section 2(1)(d). The DPC also decided that a contravention of Section 2C(2) of the Data Protection Acts 1988 and 2003 had occurred. This provision requires a controller to take reasonable measures to ensure that its employees and other persons at the place of work are aware of and comply with security measures. The lack of agreed procedures and in-depth policies in place between the RIA and Aramark relating to the transfer of personal data over a network led to this decision.

This case illustrates the unintended and unforeseen consequences which can result from an absence of clear, documented policies and procedures governing the transmission of personal data over a network. In this case, that failure was compounded by the further failure by the RIA to also have a written agreement in place which clearly set out the parameters of Aramark's instructions to process personal data on behalf of the RIA. As this case demonstrates, such failures by a controller to comply with its data protection obligations are not just administrative or regulatory breaches but can result in grave incursions into an individual's Charter protected right to protection of their personal data which otherwise should have been avoidable.

CASE STUDY 6: The importance of data controllers having appropriate mechanisms in place to respond to access requests and document compliance

We received a complaint from a data subject concerning the alleged failure of eir to comply in full with an access request. The complainant advised us that in response to his access request he had received from eir what he described as *"a bundle of random pages of information without any explanation of content"*.

In the course of our investigation we established that eir was in fact seeking to rely on certain statutory exemptions to the right of access. However in its response to the requester's access request, it had not referred at all to the fact that it had withheld certain personal data. It was only in communications with eir, during the course of our investigation, some five months after eir's receipt of the access request, that eir indicated that they were withholding personal data based on exemptions and outlined the details of the exemptions relied on by reference to an attached list.

In the course of our investigation it also became apparent that eir was unable to determine what personal data had actually been provided to the complainant as it had not retained a copy of the personal data which had been provided. As a consequence of the lack of records kept on the personal data which had been released, eir was also unable to identify what personal data had been withheld/ not provided either in reliance on an exemption under the Data Protection Acts 1988 and 2003, or otherwise.

We pointed out to eir that it would be difficult to see how eir would be in a position to provide clarification to us as to their purported application of any statutory exemption to this particular access request given that they were not clear on what personal data had been provided to the complainant in the first place. We accordingly directed eir to re-commence the process of responding to the access request afresh. We specified that in doing so, eir should:

1. Examine its systems, both manual and electronic and carry out a review of all the personal data held by it relating to the complainant in manual and electronic form;
2. Write to the complainant within a period of not more than fourteen days of the date of our request, responding to the substance of his access request in accordance with the provisions of Section 4 of the Acts. In so doing, we required that eir provide access to all personal data held or controlled by it, while also explaining to the requester the reason for the re-issue to him of personal data which had already been provided, i.e that eir was unable to determine what personal data had already issued to him. We also directed that in this response, eir also provide the requester with a statement of the reasons for the refusal to provide access to any personal data, identifying any statutory exemption relied on by eir and the basis on which eir contended that such exemption(s) applied in this case. Finally we required that eir's letter to the requester should be copied to us.

While ultimately the complainant in this case withdrew his complaint against eir, the issues identified during the course of our investigation underline the critical importance of data controllers having adequate organisational and operational mechanisms to allow them to comply with their statutory obligations with regard to access requests. However, it is equally important that a data controller is able to post facto demonstrate (where required by the DPC, such as in the context of a complaint) compliance with its obligations. A data controller must be able to justify decisions it has taken to deny access to personal data in reliance on one or more statutory exemptions. As a basic starting point of

being able to provide justification as to the position taken in relation to a request by a data subject to exercise a right, data controllers should have appropriate record keeping systems and processes in place. These mechanisms should allow them to track and produce copies of any correspondence exchanged with a data subject in relation to an access request or request to exercise any other data protection right.

This case study also underscores the fact that the right of an individual to access personal data held about them is not just about being provided with access to the data itself. Importantly it is also concerned with sufficient, meaningful information being given to the data subject so that they can understand, amongst other things, what personal data is processed about them, in what circumstances and for what purposes. In this case the provision of a bundle of unexplained documents in response to the access request failed to satisfy the minimum requirements applicable to eir as a data controller under Section 4 of the Data Protection Acts 1988 and 2003, ultimately causing confusion for the data subject and prompting a complaint to the DPC.

Appendix III
Data protection case law of the Court of Justice of the European Union

C-498/16, Schrems v Facebook Ireland Limited (Judgment of 25 January 2018)

Mr. Schrems, who is resident in Austria, brought data protection proceedings against Facebook Ireland Limited before the Austrian courts, invoking consumer law to ground his claim in that country. Seven other Facebook users who live in Austria, Germany and India purported to assign their claims to Mr. Schrems for the purposes of the same proceedings.

Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ('the Brussels I Regulation') states that defendants must, in principle, be sued in the courts of the Member State in which they are resident or have their registered office. This requirement is subject to the exception that consumers may sue in the country in which they are domiciled.

The Supreme Court of Austria made a reference for preliminary ruling to the CJEU to clarify the conditions under which the consumer forum may be invoked.

Facebook argued that:

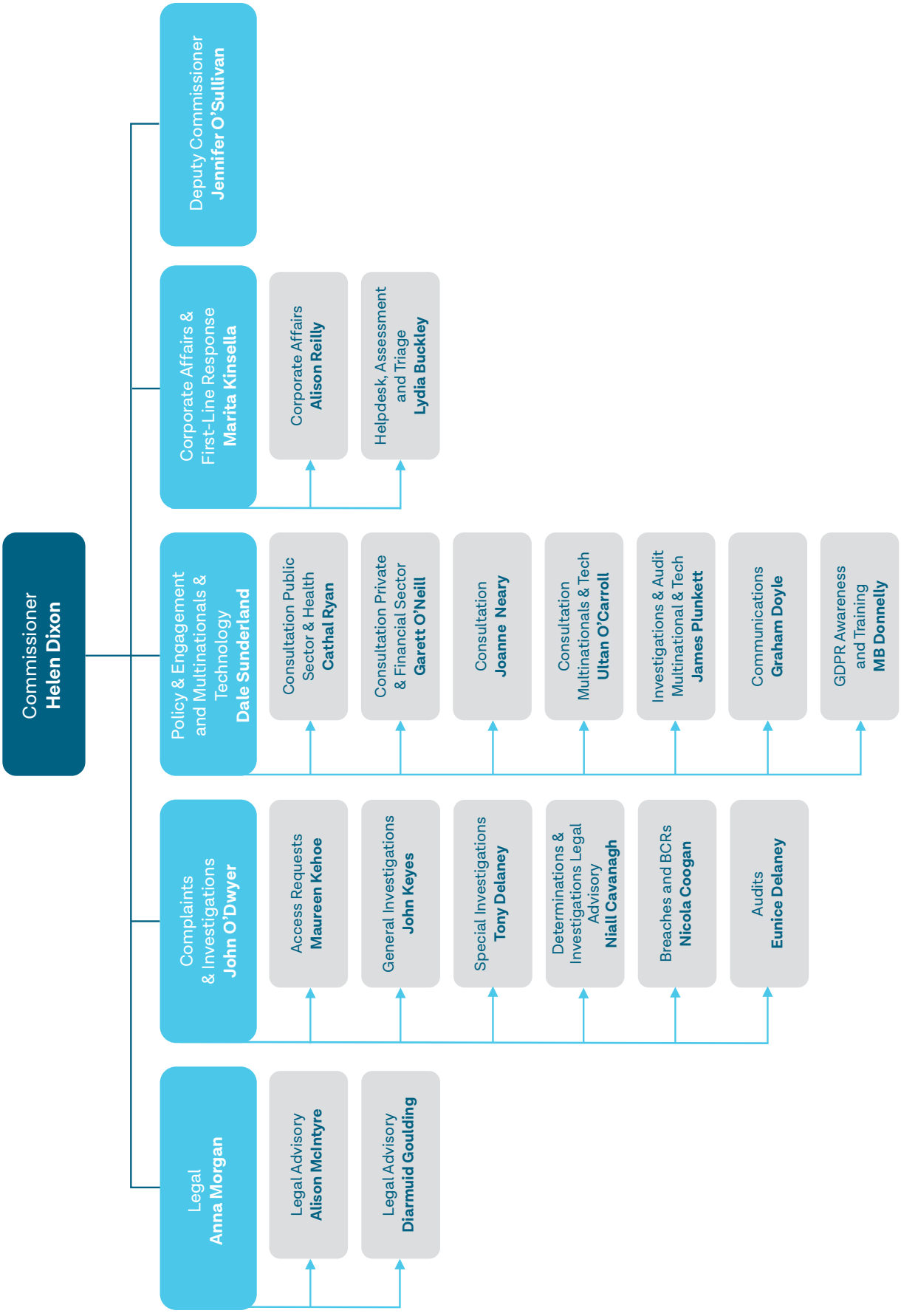
- Mr. Schrems, by using Facebook also for professional purposes (in particular by means of a Facebook page designed to provide information on the steps which he is taking against Facebook), could not be regarded as a consumer; and
- The consumer forum is not applicable to the assigned claims since such jurisdiction is not transferable.

The CJEU ruled that:

- Mr. Schrems' activities as a campaigner and academic do not result in the loss of his status as a 'consumer' with respect to Facebook, and so he was entitled to take the proceedings in Austria; however
- Mr. Schrems' status as a consumer under the Brussels I Regulation does not extend to other persons, as these people were not parties to the contract in question in the proceedings.

Therefore, Mr. Schrems was entitled to bring an individual action against Facebook Ireland Ltd in Austria, but was not entitled to represent other consumers in a class action before the Austrian courts.

Appendix IV
Organisation Chart



Appendix V
Statement of Internal Controls

Purpose of this Statement of Internal Controls

With the commencement of the Data Protection Act 2018 on 25 May 2018, a new Data Protection Commission was established under section 10 of the Act, and in accordance with section 14, all of the functions of the Data Protection Commissioner were transferred to the new Commission.

In accordance with section 66 of the Data Protection Act 2018, the Commission is required to prepare a final Report in respect of the office of the Data Protection Commissioner covering the period 1 January 2018 to 24 May 2018.

This Statement of Internal Controls has been prepared as a final Statement in respect of the Data Protection Commissioner's office, covering the period 1 January to 24 May 2018.

Scope of Responsibility

On behalf of the office of the Data Protection Commissioner, 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 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 Data Protection Commissioner for the period 1 January to 24 May 2018 and up to the date of approval of the financial statements.

Capacity to Handle Risk

The office of the Data Protection Commissioner reports on all audit matters to the Audit Committee in the Department of Justice and Equality. The Audit Committee in the Department of Justice and Equality met on two occasions between 1 January and 24 May 2018. The office of the Data Protection Commissioner's senior management team acts as the Risk Committee for the body. Senior managers from the Office attended a meeting with the Department of Justice and Equality in 2017 to discuss audit and risk issues relating to the body.

The Internal Audit Unit of the Department of Justice and Equality carries out audits on financial and other controls in the office of the Data Protection Commissioner. It carries out a programme of audits each year.

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

Risk and Control Framework

The office of the Data Protection Commissioner has iThe office of the Data Protection Commissioner has implemented a risk management system which identifies and reports key risks and the management actions being taken to address and, to the extent possible, to mitigate those risks.

A risk register is in place which identifies the key risks facing the office of the Data Protection Commissioner and these have been identified, evaluated, and graded according to their significance. The register is reviewed and updated by the senior management team on a quarterly basis. The outcome of these assessments is used to plan and allocate resources to ensure 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 which 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 Department of Justice and Equality provides the office of the Data Protection Commissioner with ICT services. They have provided an assurance statement outlining the control processes in place in 2018 in respect of the controls in place;
- there are systems in place to safeguard the office of the Data Protection Commissioner's assets. Control procedures over grant funding to outside agencies ensure adequate control over approval of grants and monitoring and review of grantees to ensure grant funding has been applied for the purpose intended; and
- the National Shared Services Office provide Human Resource and Payroll Shared services. The National Shared Services Office provide an annual assurance 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 Department of Justice and Equality's Internal Audit Unit;
- reporting arrangements have been established at all levels where responsibility for financial management has been assigned; and
- there are regular reviews by senior management of periodic and annual performance and financial reports which indicate performance against budgets/forecasts.

Procurement

I confirm that the office of the Data Protection Commissioner has procedures in place to ensure compliance with current procurement rules and guidelines and that during the period from 1 January to 24 May 2018 the Office of the Data Protection Commissioner complied with those procedures.

Review of Effectiveness

I confirm that office of the Data Protection Commissioner has procedures in place to monitor the effectiveness of its risk management and control procedures. The office of the Data Protection Commissioner'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 senior management team. The senior management within the office of the Data Protection Commissioner is responsible for the development and maintenance of the internal financial control framework.

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

I confirm that the office of the Data Protection Commissioner conducted a review of the effectiveness of the internal controls for the period 1 January to 24 May 2018. It should be noted that this extended beyond financial controls and examined ICT controls, management practices and other governance processes.

Helen Dixon
Data Protection Commissioner

Appendix VI
Energy Report

Overview of Energy Usage 1 January – 24 May 2018

Dublin

21 Fitzwilliam Square

The office of the Data Protection Commissioner in Dublin is based at 21 Fitzwilliam Square, Dublin 2. As of 24 May 2018, there were 37 people accommodated in this building. From 1 January to 24 May 2018 the sources 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.

Regus Building

To accommodate an increase in staff the previous year the DPC took out a short term office agreement for additional space in the Regus Building, Harcourt Road, Dublin 2 which continued into 2018. By 24 May 2018, there were 29 people accommodated in this building as an interim measure prior to the finalisation of a larger Dublin premises to accommodate Dublin DPC staff later in 2018. The DPC's energy usage for this building is not 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. As of 24 May 2018, 29 members of staff were accommodated in this building. The main use of energy in the Office was for gas and electricity for heating, lighting and other uses.

As of 24 May 2018, 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 our energy usage in compliance with the European Communities (Energy End-use Efficiency and Energy Services) Regulations 2009 (SI 542 of 2009).

The average energy usage for the office from 1 January to 24 May 2018:

Dublin office:

Usage	
Non-electrical	0
Electrical	18,457 kWh

Portarlington office

Usage	
Non-electrical	25,943 KwH
Electrical	18,239 KwH

The DPC has continued its efforts to minimise energy usage by ensuring that all electrical equipment and lighting are switched off at close of business each day.

Appendix VII
Financial Statement for the period from 1 January to 24 May 2018

The Account of Income and Expenditure for the period from 1 January to 24 May 2018 will be appended to this Report following completion of an audit in respect of that period by the Comptroller and Auditor General.

Special Report
Thirty Years of Data Protection in Ireland

Bob Clark (Professor Emeritus, School of Law UCD; Consultant to Arthur Cox, London and Dublin)

(The views expressed in this opinion piece are personal to the author and should not be taken as representing the views or position of the Data Protection Commission on any matter discussed in this article).

The Origins of Irish Data Protection Legislation

Data Protection laws are intended to provide human beings with specific rights and remedies that give practical meaning to sweeping declarations in International Conventions, treaties and fundamental principles of law concerning rights to privacy, legal due process and even the right to life itself. This later claim may strike some readers as being something of an overstatement but it is no coincidence that the most important organisation to foster privacy in general and data protection in particular, the Council of Europe, was established in 1949 with the horrors of the Second World War being fresh in the mind of European politicians and lawmakers. The European Convention on Human Rights followed on from the establishment of the Council of Europe one year later. The 1950 Charter recognises rights to a number of important rights such as the right to life (Article 2), a fair trial (Article 6), privacy and family life and correspondence (Article 8) and freedom of expression (Article 10). These Convention rights, which reflect the 1948 Universal Declaration of Human rights, form the basis upon which the European Court of Human rights may bring recalcitrant Council of Europe Member States into line with human rights standards. While an adverse finding that national legislation is deficient may be a matter of national embarrassment, to say the least, it is through the rulings of the European Court of Human Rights, and, latterly, the Court of Justice of the European Union (CJEU) that social and fundamental rights may be created and vindicated. In Ireland, the Airey ruling in 1979 on access to the courts, and the Norris ruling in 1988 on the criminalisation of homosexuality were landmarks in Irish civil rights. Although Germany, one of the losing states in World War II was unable to fully participate in the Council of Europe's foundation — West Germany became a Member one year after the State, the Federal Republic of Germany, was founded on May 23, 1949. But the pre-war and war years were a significant factor in stimulating the political and religious freedoms debate surrounding privacy, as a human right, in Germany in particular. The 1933 to 1945 period was one in which citizen surveillance and the subordination of democratic values to the leader principle — Führerprinzip — could result in widespread abuses of data collected on religious groups, homosexuals and certain ethnic groups, often by misuse of census and other data collected during the Weimar years of 1918 to 1933. The work of the Gestapo and the use of informers also contributed to the holocaust and other criminal acts, by citizens, against other citizens, has remained deeply troubling in Germany: even after 1949 the German Democratic Republic continued with this programme of mass surveillance.[1] In West Germany the various states, or Laender, set up their own rules concerning the use to which local administrations could put new data processing technologies. The Laender of Hesse Data Protection Act of 1970 was the first legislative text to impose a confidentiality of personal data rule. As Herbert Burkert,[2] one of the leading figures in promoting data protection rules in Europe has written, the 1970 Act, which concerned automated processing exclusively within the public sector and did not generally require data processors to register, was described as the Hesse:

""Datenschutzgesetz" (literally translated as Data Protection Act", it was a misnomer, since it did not protect data but the rights of persons whose data was being handled. But misnomers tend to have a high survival rate.

This legislation also set some basic themes for the forthcoming legislation in Europe:

(a) the negative default rule

The processing of personal data was seen as interference per se that needed legitimization.

(b) the rights of the data subject

For the first time, data subjects had a right of access to information relating to them without the need to show any reason as to why they wanted access.

(c) the omnibus approach

1 Hogan J. in Schrems v Data Protection Commissioner [2014] IEHC 310 alluded to the need to counteract the tendency of the State to seek to exercise mass surveillance of telecommunications especially in the home, remarking that (para. 53):

"Such a state of affairs – with its gloomy echoes of the mass state surveillance programmes conducted in totalitarian states such as the German Democratic Republic of Ulbricht and Honecker — would be totally at odds with the basic premises and the fundamental values of the Constitution: respect for human dignity and freedom of the individual (as per the Preamble); personal autonomy (Article 40.3.1 and Article 40.3.2)".

2 Burkert, Privacy – Data Protection, A German/European Perspective available at www.mpg.de/sites

Although — due to reasons of legislative competence — the Hesse act could not cover the private sector, it set out to regulate all of the state public sector (within its competence).

(d) the establishing of a privacy protection institution".

The German models, spawned by the Hesse text ultimately led to the **Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January 1981, and for that purpose to regulate in accordance with its provisions the collection, processing, keeping, use and disclosure of certain information relating to individuals that is processed automatically (the Strasbourg Convention).**

Ireland and Privacy Rights

As one of the 10 founding members of the Council of Europe, Ireland was of course familiar with the broader European context within which fundamental freedoms were a necessary part of post-war reconciliation. Some of the provisions in the European Convention on Human Rights were reflected in Irish Constitutional Law but the right to privacy in Article 8 was not reflected in the text of the 1937 Constitution. In subsequent litigation privacy as an unenumerated (i.e. unwritten right) was identified as a right to **marital** privacy in the 1974 case of **McGee v. Attorney General**. Later cases point up the difficulties of reconciling this marital privacy right with other fundamental freedoms: **I O'T v. B** (1998). In 1987 a broader statement on privacy rights in the context of rights of communication were provided by the President of the High Court in **Kennedy & Arnold v Attorney General**.[3] The decision in **Kennedy & Arnold** appeared some months before the publication of the Data Protection Bill 1987, and in some ways the fact that the complainants were able to recover damages for the infringement of privacy rights afforded to citizens under the Constitution a significant development, viewed in the light of the failure of the Oireachtas in the Data[3] Protection Act 1988 to provide a damages remedy when a person finds that rights have been infringed but no financial loss has been suffered. The main reason why the 1981 Strasbourg Convention was ratified cannot be said to be a Governmental conversion to the cause of personal privacy but the realisation that the Strasbourg Convention had to be ratified as a matter of commercial expediency. If Council of Europe Member States did not ratify the Convention the Article 12 prohibition on exporting personal data to non-contracting parties would interfere with data flows. In a phrase commonly used at the time, a *"data haven"* could not be allowed to acquire competitive advantages. A "data haven" became a pariah state. Indeed, during the debates on the 1987 Bill it was argued that the Bill was a necessary measure if the proposed Financial Services Centre was to turn Ireland into an International Finance Services hub.

The Data Protection Act 1988

The 1988 legislation remained largely in force up until the 2018 Act was introduced although it had been amended on many occasions, most notably in the Data Protection (Amendment) Act 2003, intended to make adjustments needed to transpose the 1995 Data Protection Directive 95/46/EC. The 1988 Act set out the general principles that data controller and data processors should observe, particularly the fair processing principle. Registration requirements were imposed although these were relaxed in later years. In terms of enforcement the 1988 Act the powers of the Data Protection Commissioner (established in the Act) consisted of a duty to investigate complaints, in which sat alongside powers to seek to mediate agreed solutions to disputes. Powers to prosecute for offences were found in the Act, particularly sections 16 and 19.[4] Separate offences in relation to electronic direct marketing have been in place as a result of the transposition of telecommunications privacy Directives since 2003 and remain in force today.[5] There are no provisions in the 1988 Act, or the 2003 Amendment Act that provide a role for the Commissioner in relation to civil remedies. This was addressed in section 7 of the 1988 Act which provides that a duty of care is owed by data controllers and data processors to individuals in regard to the collection and use of personal data. The scope of section 7 was further limited by judicial interpretation of section 7, as we shall see.

Successive Data Protection Commissioners have adopted a threefold definition of their role as Commissioner under the Acts: the Commissioner has:

- An Ombudsman Role;
- An Enforcer Role;
- An Educational Role.

The Commissioner as an Ombudsman and Educator

The educational and ombudsman role of the Commissioners needs to be appreciated. In the early years the enforcer role was subordinate, often because enforcement in civil actions and prosecutions is an expensive business. For the sake of illustration it is necessary to consider one of the success stories that attach to activities of the Data Protection Commissioner. Some dubious data capture techniques were a feature of

3 [1987] IR 587; **Schrems v. Data Protection Commissioner** [2014] IEHC 310; Herrity v. Associated Newspapers (Ireland) Ltd. [2008] IEHC 249 holds that illegal telephone tapping and publication of content by the print media cannot be defended via Article 10, freedom of the press. Damages for privacy breach of €90,000, including punitive, were awarded.

4 See for example breaches by private investigators who seek to access personal data for use by insurance companies in defence of claims; Case Study 1 of 2012 and Cast Study 1 of 2016.

5 SI No. 535 of 2003, transposing Directive 2002/58/EC; SI No. 311 of 2011 updates the unsolicited communications provisions in Regulation 13. See Case Study 12 of 2017 **(Virgin Media** – telephone calls): Case Study 13 of 2017 (**River Medical** – unsolicited marketing emails).

direct marketing organisations and a diverse range of communal entities such as banks and supermarkets. The use of free prize draws, the collection of personal data by way of customer loyalty schemes and reward programmes, without informing individuals that there would be subsequent use of personal data so captured, had long been a matter of consumer complaint and Commissioner condemnation, but recent annual reports do not contain instances of this kind of practice. In contrast, the United States of America has no federal legislation which regulates the activities of consumer data collection brokers. This has proved extremely problematical for U.S. college students who, perhaps unwittingly, participate in data capture practices conducted on campus with the consent or participation of college authorities, who often sell-on student personal data that has been compiled through SAT or PSAT admission testing. The absence of any meaningful and uniform means of prohibiting capture and sale of minor and student data, or indeed, any national body in the USA with the power to intervene or impose sanctions upon unethical (if not illegal) practices[6] stands in contrast to European legislation which clearly prohibit marketing practices of this kind. However, in Ireland, new forms of illegal data capture do emerge. The Data Protection Commissioner has noted that the harvesting of email addresses and text numbers for direct marketing represents *"a disturbing trend of commercial entitles sourcing mobile numbers of private individuals from websites or from other published sources for the purpose of using these numbers to market their own products"*.[7] The correct response to persistent misuse is a criminal prosecution.[8]

The office of the Data Protection Commissioner

Ireland has been fortunate in being able to appoint persons of outstanding merit to the post of Commissioner. The first Commissioner, Donal Lenihan was a senior figure in the Department of Justice and he had represented the State at international gatherings on data protection for several years before his appointment in 1988. Donal developed a deep knowledge of the legislation and he was responsible in large part for the drafting and parliamentary oversight of the journey of the Data Protection Bill 1987 onto the Statute Book. The legislation was not widely understood and he was tireless in the early years in attending conferences, and through his lectures and talks, in providing companies and individuals with information and advice on both the legislation and its practical implementation. Donal Lenihan set the template for data protection as being a consultative and educational process rather than an adversarial mechanism that would almost invariably, require judicial intervention.[9] Like Donal, the second Commissioner Fergus Glavey was a career civil servant who brought the application of data protection principles into areas of information technology applications that were unforeseen in 1988. Fergus Glavey was the first Commissioner to see the role as one in which *"information privacy"* rather than *"data protection"* had to be promoted by his office. Fergus served as Data Protection Commissioner for a full seven year term from 1993 to 2000. Fergus Glavey, like his predecessor, was required to administer an office with inadequate resources.[10] In September 2000 the government appointed Joe Meade to be the third Commissioner. Joe Meade came from a finance background with posts in the Office of the Comptroller and Auditor General and the European Court of Auditors on his CV. Joe Meade served as Commissioner until he was appointed as Financial Services Ombudsman in May 2005. Joe Meade proved to be an extremely effective appointment, charged as he was with pushing through the 2003 legislation. The issues that he sought to progress included the use of powers in telecommunications legislation to require data retention to extend beyond data protection requirements and a Judicial Review of Ministerial power was contemplated with Joe Meade being the Complainant. Seeing Joe Meade in action before an audience was always a joy. His (softly spoken) advices and instructions to high-powered executives and their financial and legal advisers could transfix an audience and he left no-one in any doubt that he meant what he said. Billy Hawkes was Joe Meade's successor and he served until 2014. Billy was, like his predecessors, an enthusiastic promoter of the data privacy cause; the ability to manage an office, concentrate on a number of breaking issues, which necessitated interaction with other Civil Servants and Departments, became a very important feature of the Commissioner's work. Data audits and the data breach reporting requirements were very significant developments during Billy Hawkes' watch. Most noteworthy, the migration of technology companies to Dublin as the European capital of choice created resourcing and other challenges such as the training up and retention of expertise within the office. A brief snapshot of how the office has generally struggled along on inadequate financial resources is now timely. In 1990 there were six staff; in 1995 staff levels had risen to eight but by 2000 staff levels had fallen to seven. By 2006 there were 22 members of staff, the office having been moved via the decentralisation process to Portarlington. Appointments to the office increased in following years with specialists in technology and legal affairs being recruited in 2012.

The fifth, and current Data Protection Commissioner, took up her post in late 2014. Helen Dixon has established herself as a worthy successor to Billy Hawkes and her other predecessors and her international profile

6 "Data Miners Prey on Students" New York Times International July 31 2018: One student is quoted in the article as remarking that "It wasn't like I sought out filling in my information for the College Board to sell to other companies.... you are giving them the liberty to profit off your information"

7 Case Study 5 of 2009

8 Case Study 9 of 2009; Case Study 12 of 2012; Case Study 12 of 2013

9 Donal Lenihan was appointed on July 22, 1988, serving until June 7, 1993.

10 Fergus Glavey was particularly interested in the Europol initiative, serving as Chairman of the Joint Supervisory Body for the years 1998 to 2000

and reputation is noted in an interesting article in the **Financial Times**.[11] Speaking of the 2013 Schrems Complaint in 2013 the article states:

> *"Schrems sent the complaints to the Irish data protection commissioner in Portarlington, a town with a population of 8,000. From a modest office above a supermarket, the Irish DPC was responsible for regulation all the tech companies and nominated their Dublin-based subsidiaries as "data controllers". Despite its role protecting millions of EU citizens, the commissioner had just 26 staff at the time.*
>
> *Today, the DPC has more than 90 staff and its budget has increased more than fivefold since 2011. A spokesperson says that Helen Dixon, the commissioner appointed in 2014 has led a "widely acknowledged transformation of the Irish DPC"".*

Caselaw on the meaning of personal data

The 1988 Act and the 2003 Amendment Act, in terms of the general principles that were transposed into Irish domestic law, tended to follow the provisions in the 1981 Strasbourg Convention and the 1995 Directive. Several judges have commented on the lack of detail that the 1988 and the 2003 Acts contain on key issues. In some respects such criticisms are unfair insofar as any departure in language from international principles and standards, in a search for greater clarity, runs the risk of bringing on a challenge that the domestic law fails to correctly meet the States' international obligations and/or is an incorrect transposition of a European Council Directive, for example. Case law has provided clarification on a number of issues of definition and the necessary standards that the Data Protection Commissioner must meet. Irish courts have been asked to consider what *"personal data"* means, or, to be more precise, whether certain materials or data constitute personal data. The decision of the Circuit Court affirmed on appeal by the High Court, in **Dublin Bus v. Data Protection Commissioner**[12] is noteworthy for clarifying a number of issues. Firstly, the case is authority for the proposition that CCTV footage which recorded an accident that occurred on a Dublin bus on which the complainant was travelling could constitute personal data. Secondly, there is an important difference between the attitude of the English courts and the Irish courts on the possibility that a complainant might legitimately use the 1988 Act to seek to access personal data as part of some extraneous exercise such as personal injury or breach of contract litigation. In England the Court of Appeal has considered that data protection access requests need not be complied with when an access request is made to assist in obtaining discovery of documents. Dublin Bus had argued that CCTV coverage was provided on buses solely to allow Dublin Bus to defend claims for personal injury. Both the Circuit Court and the High Court drew attention to significant differences between Irish law and the UK data protection legislation, Hedigan J. in particular holding that as data access of an individual to their personal data is a fundamental right, any arguments as to the interpretation of an exception thereto shall be narrowly construed.[13] However, in litigation between Peter Novak and the Data Protection Commissioner over an access request made by the complainant and information held by PwC, a former employer of the complainant, the High Court has ruled[14] that the records kept by PwC, which related to the way in which two audits had been conducted by PwC, the complainant at that time being a trainee engaged in the audit process, was not personal data. Coffey J. agreed with the Data Protection Commissioner:

> *"specifically, there appears to be nothing in the material that relates to the appellant [Nowak] as an identified or identifiable natural person which engages his right to privacy or which could, in any meaningful way be amenable to objection, ratification or erasure under the provisions of the [1988] Act".*

Personal data has also been held not to exist simply by virtue of the complainant being informed verbally of certain facts relating to an individual alleged to be in an email when that email was not held on an automated system. Nor could the information come within the definition of manual data, consisting as it did of information that could not be said to be part of a relevant filing system.[15]

The Schrems and Facebook Litigation

As recently as August 2012, it was possible to express the view in the High Court that *"there is very little jurisprudence on Data Protection Law in this jurisdiction".*[16] This was undoubtedly correct. There had been some earlier case law that was concerned with the jurisdiction of the Circuit Court in relation to section 26 appeals but it is only in recent years that Irish courts have had to consider a quite bewildering *"array of data protection issues"*. Some of these cases involve issues of interpretation, exploring the meaning to be gleaned from terms such as *"personal data", "disclosure"* and *"sensitive personal data"*. But undoubtedly the most profound shock to the Irish legal system in regard to data protection enforcement is to be found in Costello J.'s judgment in **Data Protection Commissioner v. Facebook Ireland Ltd, and Another.**[17]

11 **"Max Schrems**: the man who took on **Facebook** – and won" Financial Times April 5, 2018 **(Hannah Kuchler**

12 [2012] IEHC 339

13 [2012] IEHC 339; see also Case Study 5 of 2012 at [2012] IEDPC 5

14 **Nowak v. Data Protection Commissioner and PwC** [2018] IEHC 117

15 **Shatter v. Data Protection Commissioner and Another** [2017] IEHC 670. This case is one in which the most likely data controller, the **Garda Commissioner**, was not a party to the appeal because of doubts about the existence of a Garda file or record of any kind.

16 Hedigan J. in Dublin Bus v Data Protection Commissioner [2012] IEHC 339

17 [2017] IEHC 545 (the Standard Contractual Clauses Reference and CJEU of 3/10/2017)

We will look at the actual decision and the aftermath of Costello J.'s October 3, 2017 ruling in a moment, but it is evident that because of the pre-eminent position of Ireland as the location of choice for most software and new media European headquarters — whether because of English language competences, tax advantages and so on — we are going to see Irish data protection disputes, and the consequences therefrom, creating profound challenges in the years ahead. In turning to examine the **Schrems** and **Facebook** litigation, this writer must seek to elicit the forbearance of readers who may be tempted to see this treatment as simplistic: indeed it is. Consideration of space make it impossible to effectively summarise these complex issues. The October 3, 2017 judgment itself is 76 pages long. Brevity is not generally to be expected of lawyers!

While at first blush the issues raised during the Facebook Reference case of 2017 may appear to be rather technical ones — could the Irish High Court seek preliminary rulings on whether three European Commission decisions on standard contractual clauses (SCC) that had been approved for data transfer purposes — Costello J. gave a ruling on the wider importance of the case in almost Jeffersonian terms:

> *"The case raises issues fundamental to democratic societies and the balance to be achieved in respect of sometimes competing rights, values and duties. It concerns the right to data privacy which is recognised as a fundamental right and freedom by the Charter and the TFEU. It also concerns the right, indeed the duty of the State to protect itself and its citizens from threats to national security, terrorism and serious crime. A degree of surveillance for the purposes of national security, counter-terrorism and combating serious crime is vital for the safeguarding of the freedoms of all citizens of the Union. This necessarily involves interference with the right to privacy, including data privacy.*
>
> *A central purpose of the European Union is the promotion of the peace and prosperity of citizens of the European Union through economic and trading activity within the Single Market and globally. The free transfer of data around the world is now central to economic and social life in the Union and elsewhere.*
>
> *The recent history of our continent has shown how crucially important each of these objectives is to the wellbeing of the people of Europe. Damage to the global economy has resulted in very real detriment and hardship to millions of Europeans. International terrorist atrocities have been and continue to be perpetrated in many Member States of the European Union. There are many who experienced the corrosive effects of widespread state surveillance upon their private lives and society in general who regard preservation of the right to privacy, including data protection, as fundamental to a democratic society".*

Seen in this light the **Schrems** complaint takes on a more elemental perspective. The European Commission has approved standard contractual clauses that allow the export of personal data to states/jurisdictions outside the Union. The **Schrems** complaint was that the Wikileak/Snowdon revelations suggested that in the USA the privacy interest is subordinated to national security in an unbalanced fashion. The facts disclosed that personal data exported from within the EU by Facebook Ireland to its USA based parent company was available and/or disclosable to the National Security Agency, with Federal US law allegedly failing to provide a data subject with adequate remedies and procedural mechanisms to EU citizens, contrary to Articles 7 and 8 of the Charter of Fundamental Rights of the EU (private and family life protection and data protection rights respectively). Earlier Irish and CJEU decisions involving Schrems, Facebook and the Data Protection Commissioner had established that a complex relationship between national supervisory authorities (such as the Data Protection Commissioner) the relevant national Courts, the European Commission and the CJEU came into play when objections to actual or proposed transfers of personal data were made. It was incumbent upon the Data Protection Commissioner to investigate a data transfer complaint, notwithstanding the presence of a European Commission decision under Article 25(6) of Directive 95/46/EC. Although the CJEU alone could declare an EU decision such as the Safe Harbour decision of 2000 to be invalid, the national supervisory authority should be vested with sufficient capacity by the national legislature to engage in legal proceedings where the investigation concludes that the complaint is well founded. The Schrems/Facebook litigation at this time (August 2018) is still in its infancy. Costello J. on May 2, 2018, refused to agree to an application made by Facebook to stay or defer, her October 3, 2017 Order making an Article 267 TFEU reference to the CJEU, because Facebook intend to appeal against that October judgment. On July 31 2018 the Supreme Court acceded to an application to the Supreme Court by Facebook, permitting Facebook to appeal directly to the Supreme Court on a number of findings made by Costello J. in her October 3, 2017 judgment. The 10 questions that Facebook seek to explore before the Supreme Court include the alleged inappropriateness of the reference to the CJEU and perceived errors of the High Court findings on the state of US law. Clarke J. said that such grounds include the inappropriateness of finding that US law can be characterised as permitting *"mass indiscriminate processing"* of personal data. The appeal from Costello J.'s judgment will invite the Supreme Court to *"correct"* such findings. Clarke J. indicated that submissions to the Supreme Court should permit early case management to ensure that the appeal be heard before the end of 2018.[18]

18 **Data Protection Commissioner and Another v. Facebook Ireland Ltd. and Schrems** [2018] IESC 68. For a summary of the hearing before the Supreme Court see **The Irish Times**, July 18, 2018: *"Supreme Court to decide if it will hear Facebook appeal".*

Data Protection in a wider litigation context and section 7

The legislation itself contains sufficient flexibility to permit privacy rights to co-exist alongside other legal mechanisms such as statutory rights, viewed through the lens of the need to ensure that the administration of justice must be facilitated. Courts may respond to legitimate privacy concerns by way of appropriate court orders: **MB v Collins and Others**.[19] Rights to privacy and medical confidentiality are far from absolute and will yield to considerations such as the duty of law enforcement bodies to investigate possible wrongdoing; **DPP v Harty**.[20] Mutual assistance requests made for the purpose of validation of evidence obtained from Facebook and telephone traffic data are clearly permitted[21] and fingerprint data processed for compliance with a request from immigration authorities in another state has been held to constitute fair processing by the Court of Appeal in **BS and RS v. Refugee Appeals Tribunal**[22] where privacy legislation is in place, however, compliance may be carefully monitored, as in the Garda surveillance case of **DPP v. Idah**[23] statutory rights excluding access to personal data will also be respected; **BPSG Ltd v. the Courts Service and Another**.[24] A defendant brought before the courts in civil litigation must observe due process requirements but if the Data Protection Commissioner is being caught up in litigation arising out of the misuse of personal data by a data controller it may be inappropriate to join the Data Protection Commissioner as a defendant to an underlying commercial dispute: **Grant Thornton (a firm) v. Scanlon**.[25] This reluctance to involve the Commissioner is particularly evident when the Commissioner's powers are not engaged in such litigation.[26]

Irish judges have been circumspect in providing data subjects with financial redress when a data controller has failed to meet the standards required by the legislation. The 1988 Act, in section 7, created a broad duty of care for data controllers and data processors in relation to the collection or use of personal data. The section was rooted in a negligence standard, as the proviso to the section indicates. A data subject is of course entitled to seek damages by using a number of different legal claims such as defamation, breach of contract, infringement of Constitutional Privacy rights, for example, and damages in such instances may be substantial, even if no economic loss is shown.[27] In **Collins v FBD Insurance**[28] the plaintiff, who was insured with the defendant, lodged an insurance claim that was handled with less than professional care. The Circuit Court awarded €15,000 in damages. On appeal the High Court, starting from the assumption that the award was based exclusively on breach of the section 7 duty of care,[29] allowed the appeal. Feeney J. said that Irish law did not provide for payment of compensation for non-economic loss (a possible measure under Article 24 of Directive 95/46/EC)) and because section 7 did not provide for strict liability, and in the absence of a psychiatric injury, no compensable damage was suffered by Collins:

> *"The statutory position in Ireland is that no matter how blatant the breach that the person who is the subject of the breach can only receive damage on proof of loss or damage caused by the breach".*

Distress, anger, humiliation etc. is not enough. Fortunately, the GDPR permits compensation for material and non-material damage; see the Data Protection Act 2018, section 117(10). It remains to be seen whether the provisions in section 117 of the 2018 Act trigger claims to damages by disgruntled data subjects. Judges are often reluctant to open up new grounds for complaint, fearing that to do so may *"open the floodgates"* to monetary claims, a policy consideration perhaps in **Collins v. FBD Insurance** itself.

Concluding Remarks

It is impossible to do complete justice to 30 years' of data protection rights in Ireland in a short piece of this nature but, to the extent that there has been an accumulation of case law at this point, important progress in clarifying the nature of data protection rights has been achieved. Of course now, we are in a very new era. The new General Data Protection Regulation will bring new challenges, hopefully higher standards, more harmonisation and more litigation as the stakes grow higher for data controllers found to infringe. I look forward to tracking the progress!

19 [2018] IECA 142 (family law hearings and redress schemes)

20 [2016] IECA 142 (Gardaí taking blood samples from unconscious patient)

21 DPP v Moran [2018] IECA 176

22 [2017] IECA 179

23 [2014] IECCA3

24 [2017] IEHC 209

25 [2017] IEHC 648

26 McCann v J.M and Y.W. [2015] IECA 281; Shatter v. Data Protection Commissioner [2017] IEHC 670

27 See Hogan J. at paragraphs 36 to 39 of his judgement in McCann v. J.M and Another [2016] IECA 281

28 [2013] IEHC 137

29 Unfortunately, Irish law is not clear on the post contractual duty to process insurance claims in good faith; this duty, where it exists, could have allowed Mr. Collins to rely exclusively on a contract claim. His action in the Circuit Court was based in part on contract but the actual basis of the award made in the Circuit Court was unclear.

Data Protection Commissioner,
21 Fitzwilliam Square,
Dublin 2.

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

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner