Annual Report

Presented to each of the Houses of the Oireachtas, pursuant to Section 14 of the Data Protection Acts 1988 and 2003.

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

2017 was the year in which a somewhat unwieldy acronym which many had assumed was solely the concern of their legal and IT departments became a topic of frequent conversation in business, government and indeed daily life. The General Data Protection Regulation (GDPR) is nearly upon us, and even for those who understood its implications early on, 2017 was not surprisingly a year of intense activity globally in data protection and equally at a national level.

I'm very pleased to submit the Annual Report of the Irish Data Protection Commissioner (DPC Ireland) for 2017 highlighting our work this year and our priorities for the coming years. This is the fourth report I have had the privilege of presenting as Commissioner. Even in that relatively short period, the importance of our personal data, and moreover our comprehension of what it means to have our personal data collected, held, used and transferred by countless visible and invisible actors has multiplied exponentially.

While GDPR preparation dominated much of the year, DPC Ireland was also very busy on the litigation front as a party to multiple sets of proceedings in which important issues of data protection interpretation were brought before the Irish Courts for determination. At an international level, the Privacy Shield (the successor to the Safe Harbour framework for conducting EU to US transfers) was subject to its first review carried out by the European Commission and to which the Article 29 Working Party contributed. Meanwhile in the US, the Supreme Court accepted for hearing the US Department of Justice's appeal concerning its attempts to obtain, by US court warrant under the 1986 Stored Communications Act, data which is held by Microsoft on a server in Ireland. These major international data protection events are all hallmarks of the burgeoning importance of data protection and privacy as fundamental human rights, with 120 countries now having adopted data protection laws, up

from 109 in 2015.[1] And the nature of data protection as a fundamental right for Europeans is underscored by the enhanced protections for individuals under the GDPR and the concomitant increased obligations on data controllers and processors. Becoming compliant under the GDPR is far from a box ticking exercise: it will ultimately allow individuals greater control of the collection and processing of their data through a new modernised, harmonised EU legal order for data protection.

DPC continued to grow

This was the year in which DPC Ireland moved into a different gear as a data protection authority. Our increased budget for 2017 (€7.5m) allowed us to recruit extensively, adding a very strong team of new hires with a diverse range of relevant skills, bringing our numbers to 85 at the end of 2017. In fact, DPC Ireland is now among the top tier of the most highly-resourced national data protection authorities of the EU 28. These new hires were selected through targeted recruitment campaigns seeking very specific experience and skills within the legal and technical disciplines. Our increased budget for 2018 (€11.7m) is a further welcome commitment from Government to the importance of a robust data protection regime through the continued strengthening of DPC Ireland, and will allow us to recruit a further 55 staff in 2018. 2017 was also the first time DPC Ireland ran a competitive summer internship programme for law undergraduates, to great success. The internship programme attracted a large amount of interest, with three outstanding interns being selected from Trinity College Dublin and the London School of Economics and working with us over a two-month period in what was a mutually beneficial learning experience.

Implementing the GDPR requires huge changes from businesses and organisations and this is no different for a supervisory authority. From very early on, DPC Ireland adopted a systematic project management-based approach to preparing for May 2018. This involved mapping our current approach against the future approach required under the GDPR, identifying and implementing the website and case management system changes that will be required and building a blueprint that will allow us restructure, upscale and retrain the organisation. Combined in due course with the Data Protection Act 2018 which will give further effect to the GDPR in Ireland, the Irish DPC will be in a strong position to supervise rigorously and fairly while maximising the outcomes for data subjects under the GDPR.

Helping organisations prepare for the GDPR

The GDPR's focus is on demanding accountability from organisations in how they collect and process personal data. The best results for data subjects are secured when organisations of all types deliver on their obligations to be fair and transparent. In our experience as a data protection authority, few organisations disagree with the fundamental principles of data protection legislation. Quite simply they make sound business and consumer engagement sense. We have therefore focussed very significant resources in 2017 on driving awareness of the GDPR so that organisations are motivated and energised to make the necessary changes to their businesses. We firmly believe that they should see the GDPR as an opportunity rather than a challenge, and that those who can demonstrate a true commitment to data protection will be rewarded in the marketplace for their services.

[1] Greenleaf, 2017

"Data Protection Dave" (featured on page 46 of this report) was a new creation of DPC Ireland in 2017, allowing us to present the principles of privacy and data protection through a simple and accessible medium. Indeed, the videos we created have won a number of domestic and international awards in the last 12 months and have been viewed over 1.4 million times.[2]

"In-person" engagement was as important as ever during 2017 and staff from DPC Ireland spoke at a record number of conferences, workshops, GDPR roadshows and roundtables (almost 250) over the course of the year, both in Ireland and internationally. One notable highlight was DPC Ireland's staff keynoting and presenting in multiple panels and workshops at the Government's inaugural Data Summit in the Dublin Convention Centre in June 2017. Both at home and abroad, DPC Ireland also gave multiple radio, television and print media interviews. As ever, DPC Ireland responded as rapidly as possible to a very high volume of media queries from national and international press on an extremely wide range of issues, given the widespread reach and ever-increasing public and media focus on data protection and privacy concerns.

On the 25th May 2017 — exactly one year out from the GDPR — DPC Ireland published the results of an extensive awareness survey which was commissioned on GDPR preparedness amongst SMEs and micro enterprises nationally. We used these results to focus our information efforts where they were most needed but also as a platform from which to drive further general awareness of the GDPR. We prioritised the publication of content for organisations in 2017 that assists them in identifying and prioritising the steps they need to take, including a 12-step guide to preparing for the GDPR and a dedicated guide for SMEs, all published on our new dedicated microsite: www.GDPRandYou.ie.

Face-to-face meetings with a broad range of public, private and voluntary organisations in relation to their implementation of data protection legislation and in particular their preparations for GDPR-compliance were a constant feature of 2017 with over 200 consultations. In particular, the larger entities supervised by DPC Ireland have engaged extensively with us over the last year. With internet and social media companies, our priority has been ensuring that these companies have a lawful basis for data collection and provide full transparency to users so that they can understand the business model and implications of these "free services" and how their personal data is monetised and used. Driving higher standards of protection for children when using internet and social media companies has equally been a key areas of focus in advance of May 2018. In the case of Facebook and WhatsApp, DPC Ireland oversaw the delivery of a much clearer FAQ to service users spelling out how and in what instances data-sharing between the now merged entities would occur. In addition, DPC Ireland has maintained its insistence that WhatsApp's EU personal data not be shared with Facebook Ireland for ad serving and product enhancement purposes unless and until DPC Ireland is satisfied that there is a lawful basis for doing so.

International and EU Cooperation

GDPR will only heighten the importance of regulatory co-operation across borders, and DPC Ireland played an active role in deepening and strengthening engagement with our international and EU peers and stakeholders in 2017. At an EU data protection authority level, the DPC Ireland participated in all subgroups of the Article 29 Working Party (made up of all the EU data protection authorities). DPC Ireland led in a rapporteur capacity in certain critical areas such as producing harmonised guidance for stakeholders. DPC Ireland also prioritised participation in international panels and events alongside fellow data protection authorities in order to drive better mutual understanding and cooperation, contributing at events including IAPP Washington, the European Spring Conference of Data Protection Authorities in Cyprus, the Privacy Laws and Business conference in Cambridge and the International Conference of Data Protection and Privacy Commissioners in Hong Kong. DPC Ireland also spoke alongside the UK's Information Commissioner's Office at a University of London-hosted conference dedicated to *Children and Digital Rights*, emphasising the increased protections for children under GDPR. Additionally, DPC Ireland accepted the invitation of the European Data Protection Supervisor to engage with its staff in a GDPR-readiness roundtable in December alongside the Commissioner from Schleswig-Holstein in Germany and a representative of the Hamburg data protection authority. It is DPC Ireland's firm belief that the more data protection authorities in the EU and further afield know and understand each other and their methods, the more effective their trust in, and cooperation with, one another will be to the benefit of all data subjects.

[2] Irish Internet Association Net Visionary Award (winner), the inaugural ICDPPC Global Privacy and Data Protection Awards — education and advocacy category (second place) and nominated for a Spider Award.

Data Protection Commissioner Helen Dixon speaking at the 2017 Dublin Data Summit.

As in previous years, DPC Ireland engaged with our colleagues across the world in the Global Privacy Enforcement Network (GPEN) in "sweeping" a certain targeted number of websites and apps to examine compliance. This year the focus was on the clarity and transparency of privacy notices by a broad range of businesses. Arising from this work, DPC Ireland issued detailed guidance on the issuing of e-receipts by retailers and the rules they must follow in collecting shoppers' email addresses purportedly for this purpose.

Co-operation under the Memoranda of Understanding which DPC Ireland has signed with a number of non-EU authorities again provided useful opportunities to share approaches and information about some of the global breaches we investigated last year.

Litigation and Prosecutions

No summary of the work of DPC Ireland in 2017 would be complete without a reference to the *Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems* proceedings which DPC Ireland initiated in the Irish High Court in May 2016 concerning the validity of transferring personal data from the EU to the US through a commonly used legal mechanism known as Standard Contractual Clauses. The substantive hearing of these proceedings (to which the Court joined four further parties as amici ("friends of the Court"), including the US Government) ran for almost six weeks across February and March of 2017 with numerous complicated issues of EU and US law presented to the Court. If there were ever any doubts about how fast-moving an area of law data protection and privacy law is, it was demonstrated by the fact that the various parties on six further occasions following the conclusion of the trial, presented further legal and factual updates to the High Court between March and October. The judgment delivered by Ms Justice Caroline Costello on 3 October approved the DPC Ireland's request for a reference to the Court of Justice of the EU (CJEU) seeking a ruling on the validity of the Standard Contractual Clauses. That reference will be made during 2018 once the High Court has finalised the specific questions to be referred to the CJEU. We believe that the determination of these matters will ultimately assist all stakeholders in their understanding of the requirement under EU data protection law to demonstrate adequate protection in the territory to which personal data of EU persons is sought to be transferred and bring clarity to the relevant tests for comparison between the EU data protection regime and other jurisdictions.

On the subject of litigation, a judgments database on the DPC website which was launched at the end of 2016 now facilitates easier access to relevant litigation and judgments in cases to which DPC was a party. In addition to publishing the judgment in the litigation described above concerning Standard Contractual Clauses, DPC Ireland has also published a number of explanatory memoranda as well as the transcripts from the trial of these proceedings and the evidence put forward on behalf of DPC Ireland.

In 2017, the CJEU also issued its ruling in the *Nowak v. Data Protection Commissioner* case on foot of a reference from the Irish Supreme Court, in a case that concerned a request for access to an examination script produced in a professional open-book accountancy examination. The CJEU found that the examination script in this case was personal data, as would be the case for any comments from the examiner marked on the script. The Nowak

case is certainly one that gives rise again to the debate about what one academic has described as the "unfathomable scope" of data protection regulation.

A number of prosecutions were successfully pursued by the DPC in 2017 in cases involving unsolicited direct marketing and again in relation to unlawful processing of personal data by Private Investigators. Details are set out on page 65.

Key investigations

DPC Ireland commenced a number of key investigations in 2017, including into the handling of paper-based medical files of patients in public areas of hospitals and key findings from this investigation will be published in the first half of 2018. An investigation into the governance of personal data in case management files at TUSLA was commenced in the summer of 2017 with the key findings and recommendations set out on page 23 of this Report. A resource intensive investigation of potential issues surrounding the Public Services Card (PSC) has also been the subject of active work, with a view to concluding in the second quarter of 2018.

The consistent rise in the DPC's caseload over recent years continued in 2017 and a record number of complaints (2,642) were lodged and handled in 2017. 34 decisions under Section 10 were issued and a number of illustrative cases are set out in the case study section of the annual report at Appendix II. Access request complaints remained the dominant theme. The majority of complaints were amicably resolved between the parties once the DPC intervened on behalf of the data subject. However as with every year, there were cases that DPC Ireland handled where the data subjects involved remained dissatisfied with the outcome, even in some cases where the complaint in question was upheld by DPC Ireland. The majority of these cases involve issues arising as a result of the financial crash. Cases involving the transfer of loan books to new lenders and receiverships where buy-to-rent owners are involved appear in some cases incapable of being resolved to the satisfaction of the data subjects, as their fundamental grievance relates to the underlying transaction itself or the actions of the lender, rather than data protection issues per se. While inevitably personal data is transferred and processed in these circumstances, it is generally provided for in the original terms the borrower signed. In many of these cases, data protection law cannot resolve the issues at hand nor can it be used to prevent otherwise legitimate commercial transactions that were clearly provided for within the terms and conditions of the contractual relationship between the parties.

A record number of data breach notifications (2,973) were also handled during 2017 with the majority coming from the financial services sector. As we've commented before, the *mandatory* requirement under the GDPR to report data breaches posing a risk to data subjects from 25 May 2018 will reveal a far more complete picture this time next year. DPC Ireland's complex investigation into the massive data breach suffered by Yahoo! (now Oath) is now approaching completion. A central aspect of that investigation concerns the extent to which the EMEA controller (Yahoo! EMEA in Dublin) complied with its obligations to ensure that the processing of EU users' personal data by its processor, Yahoo! Inc. was sufficiently secure in terms of technical and organisational measures to safeguard the data.

Cybersecurity must now be a key priority for all organisations to maintain 'integrity and confidentiality' — particularly as this is one of the two new general principles of data protection introduced under the GDPR and against which the higher level of fines under GDPR will apply.

Contribution to Oireachtas Committees

DPC Ireland continued its important role of providing clarity on data protection requirements through appearances at a number of Oireachtas (parliamentary) committees engaged in pre-legislative scrutiny. DPC Ireland appeared before the Joint Oireachtas Committee on Finance, Public Expenditure and Reform, and Taoiseach in its pre-legislative scrutiny of the Data Sharing and Governance Bill in May 2017 and cautioned that the essential principle of purpose limitation in the use of personal data cannot simply be overridden by a Bill allowing any public bodies to share data with one another. Separately, while appearing before the Joint Committee on Justice and Equality which conducted pre-legislative scrutiny of the General Scheme of the Data Protection Bill in June 2017, DPC Ireland raised its serious concerns about proposals to retain the existing Data Protection Acts 1988 and 2003 under the GDPR framework and also the decision not to allow for administrative fines to be imposed on public bodies under the GDPR other than in circumstances where they compete with a private entity.

Public bodies must be standard bearers for the highest standards of data protection, but unfortunately numerous historical examples have shown that government departments often struggle at least as much as

private enterprises with compliance. We believe it is essential therefore that they are subject to the full extent of the new regime.

In addition to its extensive engagement with the Department of Justice and Equality providing observations and technical clarifications on what will become the Data Protection Act 2018, DPC Ireland has provided similar inputs to staff of the Department of Communications, Climate Action and Environment engaged in the EU negotiations on the new draft e-Privacy Regulation.

Interception, Retention, Oversight and Tele2

Mr Justice John Murray's Review of the Law on the Retention of and Access to Communications Data issued in October 2017. This comprehensive report provides the government with a clear roadmap to address a range of issues with existing data retention legislation. Indeed, the Government has since published a Bill that was subject to pre-legislative scrutiny at the end of 2017 which is aimed at addressing many of the issues highlighted by Justice Murray, including the requirement for judicial pre-authorisation for access to data and proactive notification to users after the fact. Oversight remains an issue that merits further scrutiny, however, as do the broader sets of issues that need to be considered around Interception. The pieces of this particular jigsaw will inevitably have to fall into place on a phased basis. There is much to address in legislative terms. Issues of institutional capacity will also have to be considered given the range and depth of the changes that need to be implemented within a short space of time. However despite the legacy and legislative challenges that lie ahead, it is the view of DPC Ireland that the Government should immediately prioritise the re-working of the existing legal framework for access to retained data. This will ensure that Ireland is compliant with the clear standards necessary for a modern system of access, built on a sound legal foundation that provides legitimacy by respecting the rights of citizens and features (amongst other things) stringent and specific judicial oversight, as well as effective avenues for redress for individuals whose rights or interests have been found to have been prejudiced. Taken together, the requirements identified by the CJEU in Tele2/Watson by reference to the Charter of Fundamental Rights of the EU, and the failings identified in the "Murray Report", mean that retaining the status quo as it presently applies in this jurisdiction is simply not an option.

Multi-disciplinary cooperation and internet company regulation

Arguably the degree of technological change continues to rapidly outpace society's understanding and discussion of its effects, but 2017 has to some extent been the year where ideas began to crystallise around how multinational internet companies need to be regulated to ensure continued innovation, while always underpinned by data protection and privacy. Coherence between data protection, competition and consumer law will be necessary to deliver a fair deal to service users. One hand cannot approve a merger without conditions while the other hand effectively has to try and block it after the fact by preventing data-sharing between the two. In an interesting blogpost in December 2017 the European Data Protection Supervisor envisaged a medium to long-term future where Europe could implement a single EU Digital Regulator across the multiple relevant disciplines. In the meantime, we have the One-Stop-Shop and GDPR to implement as effectively as we can.

The Year Ahead

The phrase "game-changer" is so frequently used that it has to some extent lost its potency. But I truly believe that May 2018 will be a seminal milestone in ensuring that the rapid technological change and importance of data in our daily lives is now backed by a transparent and flexible but robust regime for the protection of individuals. 2017 has been a year of great progress for DPC Ireland, especially towards the goal of GDPR implementation and enforcement. Hold on tight as the final countdown gets underway!

Helen Dixon
Data Protection Commissioner

Role and Responsibilities of the Data Protection Commissioner

The Data Protection Commissioner (DPC) is the national independent authority in Ireland with responsibility for upholding the fundamental right of the individual to have their personal data protected. The statutory powers, duties and functions of the DPC are as established under the Data Protection Acts 1988 and 2003, which transposed the Council of Europe Convention 108 and the 1995 Data Protection Directive. The DPC will become a 'Supervisory Authority' under the EU data protection legal framework which will apply across the EU on 25 May 2018. The new framework comprises the General Data Protection Regulation (GDPR) and a Directive (2016/680) concerning personal data processing in a law enforcement context (Law Enforcement Directive). A new Data Protection Act currently before the Oireachtas (as at February 2018) will give further effect to the GDPR in areas where national choices are permitted, transpose the Law Enforcement Directive into Irish law and give further underpinning to the structures, functions and powers of the DPC.

Using its statutory powers, the Data Protection Commissioner undertakes investigations of complaints from individuals, and identifies risks to personal data protection in a variety of public and private sector organisations through consultations with organisations processing personal data, and through on-site inspections and audits, amongst other activities. The DPC also seeks to drive better awareness of, and compliance with, data protection legislation through the publication of high-quality guidance, proactive engagement with public and private sector organisations and ultimately enforcement action where necessary.

DPC Senior Management Committee

In order to continue to implement enhanced governance structures to comply with the Code of Practice for the Governance of State Bodies, and in recognition of the significantly increased funding allocation and the rapidly-growing size of the organisation, the DPC established the Senior Management Committee (SMC) in 2016 comprising of 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. The Committee's terms of reference include: the strategic leadership, management and oversight of the organisation; monitoring performance of management and staff against the organisation's strategic and business priorities and objectives.

Our Senior Management Committee is comprised of:

1. **Ms. Helen Dixon** (Data Protection Commissioner)
2. **Ms. Anna Morgan** (Deputy Commissioner — Head of Legal)
3. **Mr. Dale Sunderland** (Deputy Commissioner)
4. **Ms. Jennifer O'Sullivan** (Deputy Commissioner)
5. **Mr. John O'Dwyer** (Deputy Commissioner)
6. **Ms. Marita Kinsella** (Deputy Commissioner)

Funding and administration

Government allocation of funding has increased significantly from €1.7 million in 2013 to €7.5 million in 2017. The DPC's funding for 2018 has once again increased to almost €11.7 million and the office acknowledges the significant increase in funding in recent years and welcomes the Government's continuing commitment to meeting the resourcing needs of the office. Dedicated funding for the DPC is channelled through the vote of the Department of Justice and Equality. These funds allows us to fulfil our mandate as the independent supervisory body in Ireland charged with upholding the EU fundamental right to data protection. The DPC also collects revenue for the statutory registration function of the office, and that revenue is remitted directly back into the exchequer. The Account of the Income and Expenditure for 2017 can be reviewed in Appendix VII.

Our increased budget for 2017 has allowed us to recruit extensively, adding specialist skills in the areas of Communications, Legal, Multinational and Technology, Investigations and Complaints. The recruitment focus of 2016 and 2017 has resulted in a significant increase of staff and this increased resourcing of the DPC will continue at a rapid pace in 2018, when the total staffing of the office is expected to rise to approximately 140 staff.

Though the DPC is an independent body, we follow the requirements set out for all public sector bodies to ensure oversight in our administrative activities. All expenditure must be accounted for to the exchequer and the Comptroller and Auditor General audit our accounts annually.

Further corporate and administrative related information is set out at the section on Corporate Affairs.

The Data Protection Commissioner's main goals for 2018

Build the capacity and capabilities of the DPC to reflect our enhanced role under the new GDPR and ePrivacy regime with a focus on:

- Engaging proactively with Government to ensure that we have the required financial and other resources, including staff and appropriate accommodation, to enable us to do our job effectively and efficiently;
- Concluding work on redeveloping our structures, processes and systems (including our ICT capabilities) to ensure our continued effectiveness under the new data protection regime; and
- Enhancing our expertise and capacity through the training, development and upskilling of staff, and the targeted recruitment of staff with specialist skills.

Close collaboration and partnership with EU and International data protection authority counterparts, and regulatory bodies in other spheres:

- 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;
- Participating effectively and constructively in the new European Data Protection Board (EDPB), with the objective of contributing to the proper and consistent implementation of the new laws and the development of common positions and responses to pan-EU data privacy developments;
- 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;
- Continuing to foster close relationships with International DPAs through forums such as the Global Privacy Enforcement Network and the International Conference of Data Protection Commissioners; and

- Promoting bilateral cooperation and information sharing by hosting delegations from EU and International Data Protection Authorities and authorising their participation in DPC audits and investigations.

Drive better data protection awareness and compliance through strategic consultation:

- 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.

Effective Oversight and Enforcement:

- 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;
- 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; and
- Driving improved compliance with data protection obligations through investigations and audits targeting high-risk and large-scale processing of personal data.

Ms. Helen Dixon

Mr. John O'Dwyer

Ms. Anna Morgan

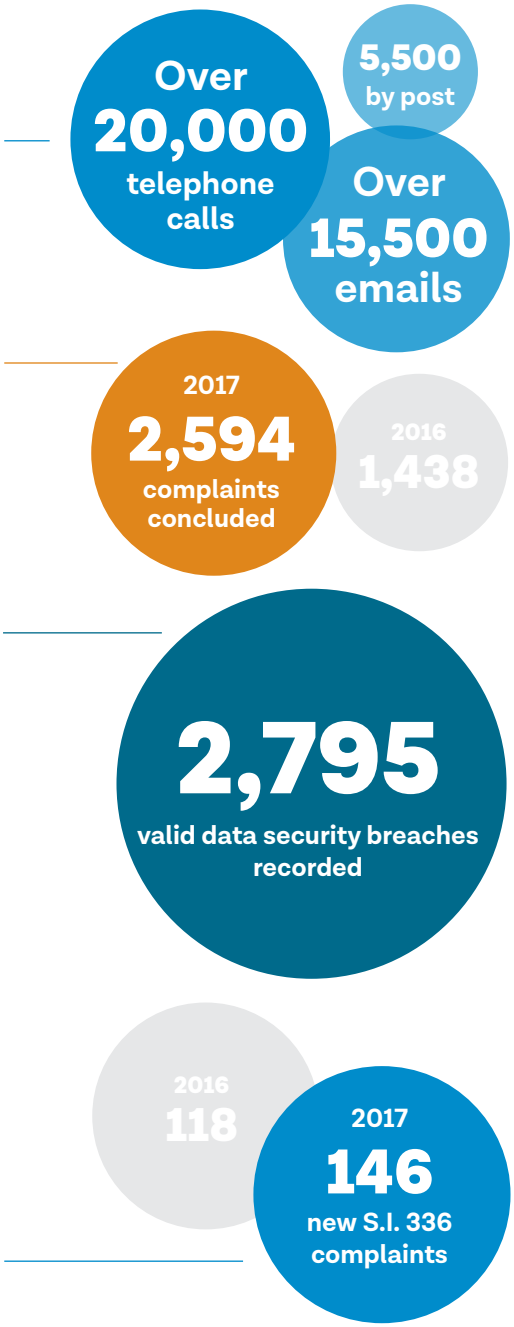
Ms. Jennifer O'Sullivan

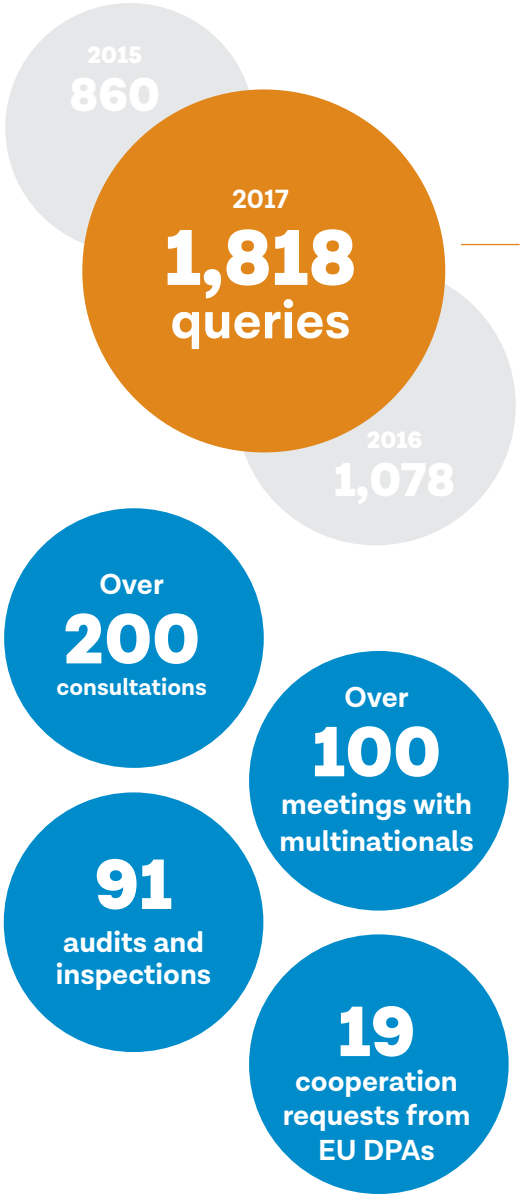
Mr. Dale Sunderland

Ms. Marita Kinsella

Review of 2017 in Brief

- In 2017, our Information and Complaint Assessment Unit received over **15,500** emails, over **20,000** telephone calls and we received almost **5,500** items via post.
- Total Complaints received in 2017 was **2,642**, up from 1,479 in 2016 (a 79% increase), with the largest single category being "Access Rights" which made up 1,372 complaints or 52% of the total.
- **2,594** complaints were concluded in 2017, compared to **1,438** in 2016.
- While the majority of complaints continued to be amicably resolved, we issued a total of 34 formal decisions in 2017.
- **21 "Right to be forgotten"** complaints were investigated. 6 of these complaints were upheld, 12 were rejected and 3 are currently under investigation.
- **2,795** valid data security breaches were recorded in 2017. This represents an increase of 26% (571) on the numbers reported in 2016.
- **The Special Investigations Unit** continued its work in the Private Investigator sector resulting in several prosecutions. It also commenced investigations in the Hospital Sector on the processing of patient data, on Tusla (the Child and Family Agency) regarding the governance of personal data concerning child protection cases and on the Public Services Card of the Department of Employment and Social Protection.
- Under the Data Protection Acts, a private investigations company was prosecuted for disclosure of data without authority and a director of that company was prosecuted for offences under Section 29. The summonses for these two cases covered 74 offences.
- 6 entities were prosecuted for offences under Regulation 13 of S.I. 336 of 2011 in respect of electronic marketing. The summonses for these 6 cases covered forty-two offences.
- **146** new complaints were investigated under S.I. 336 of 2011 in 2017 in respect of various forms of electronic direct marketing. (In 2016, the total number of new complaints investigated in this category was 118).





- General consultation queries increased significantly in 2017 to a total of **1,818** queries. This represents an increase of 69% from 1,078 queries in 2016 and an increase of 111% when compared with 860 queries in 2015.
- Over **200 consultations** were conducted with private and public sector organisations, of which the GDPR was a common theme.
- Over **100 meetings** were held with multinational companies.
- There was intensive engagement with WhatsApp and Facebook to ensure that there continued to be no transfer of user data from WhatsApp to Facebook for ads serving and product enhancement until the DPC is satisfied that there is a lawful basis for doing so.
- **91 audits/inspections** were carried out.
- **19 cooperation requests/referral** of cases from other data protection authorities were dealt with.
- In 2017, the Global Privacy Enforcement Network conducted its **5th annual Privacy Sweep**. The Irish element, conducted by the DPC as part of a worldwide sweep, included the use of e-receipts by retail companies. The Sweep found that in 94% of cases, retailers offering e-receipts to customers provided no information on their websites with regard to the processing or deletion of e-mail addresses gathered for this purpose.
- The hearing in the DPC Standard Contractual Clauses (SCCs) High Court case held in February/ March 2017. Judgment was delivered by Ms. Caroline Costello in October 2017.

- During 2017 the DPC acted as lead reviewer in relation to **14 Binding Corporate Rules (BCRs) applications** which is a doubling of our 2016 numbers.
- There was strong strategic engagement by DPC Ireland with the Article 29 Working Party with all plenary and subgroup meetings actively contributed at. DPC acted as lead rapporteur on the GDPR transparency guidance and supported the Article 29 Working Group actively in its key roles for 2017 in issuing guidance to controllers on the GDPR and in contributing to the first annual review of Privacy Shield.
- In 2017, the DPC established a dedicated **GDPR Awareness and Training Unit**, with responsibility for driving the DPC's GDPR awareness activities. Central to the GDPR awareness drive was the launch of a GDPR micro-site, www.GDPRandYou.ie, serving as a central hub for published guidance and a starting point for organisations seeking assistance with GDPR preparations.
- The DPC has maintained an active outreach schedule during 2017 and engaged with a broad base of Irish and international stakeholders. The Commissioner and her staff have spoken and presented on almost **250 occasions** in 2017, including conferences, seminars, and presentations to individual organisations from a broad range of sectors.
- Our Twitter account, @DPCIreland, created in October 2016, has shown a significant growth rate, with followers up by 200% to **3,800** by the end of 2017. Throughout the year, @DPCIreland was 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. Our Twitter account had almost **4 million impressions** for the year and a notable engagement rate of 1.5%.

Contacts, Queries and Complaints

The DPC provides a responsive and high-quality information service through our public email and telephone helpdesk service. The DPC received a record number of contacts, queries and complaints in 2017. Our Information and Complaint Assessment Unit received over 15,500 emails, more than 20,000 telephone calls and we received almost 5,500 items via post.

We aim to address all data protection queries and complaints in as short a period as possible, to the satisfaction of the querist. In many cases, this will involve providing the querist with the information and guidance necessary to enable them to resolve their data protection issue themselves with the organisation that has been controlling or processing their data as expeditiously as possible. In some instances, depending on the nature of the matter, it may be necessary for the DPC to intervene on behalf of the data subject or to initiate a formal investigation of the complaint.

The DPC received 2,642 complaints in 2017, up from 1,479 in 2016 (a 79% increase), with the largest single category being "Access Rights" which arose in 1,372 complaints or 52% of the total. The current statutory period for complying with access requests is 40 days, but this is being reduced to one month under the GDPR.

As part of the ongoing work of the DPC, the nature of queries and complaints are continuously monitored to help identify trends and patterns. The purpose of such analysis is to assist the DPC in preparing and disseminating relevant guidance and information. For example, in May 2017, the DPC issued a statement on the use of facial detection technology in advertising, after it received a number of queries from members of the public and the media on digital advertisement screens in public spaces. Concerns expressed by members of the public in relation to the Public Services Card were also noted during the year, and a statement by the Commissioner on the matter was issued in August 2017.
(See page 23 for more information)

Electronic Direct Marketing Complaints

The DPC received 215 complaints in relation to electronic direct marketing in 2017. A total of 146 new complaints were investigated under S.I. 336 of 2011 in 2017 in respect of various forms of electronic direct marketing. (In 2016 the total number of new complaints investigated in this category was 118).

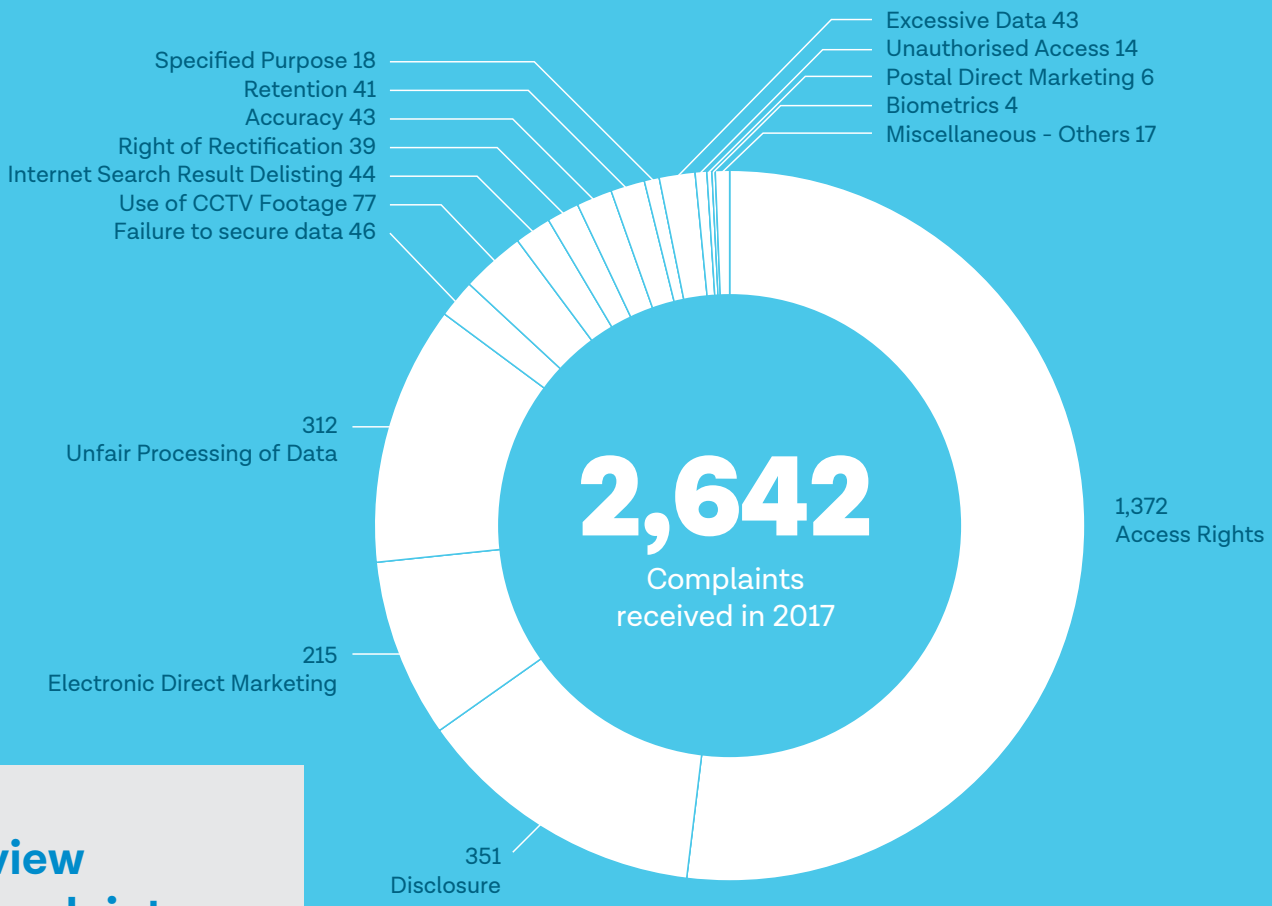
Of the 146 complaints investigated in 2017, 80 related to email marketing, 58 related to SMS (text message) marketing and eight related to telephone marketing.

The Data Protection Commissioner's office concluded 119 electronic marketing complaint investigations in 2017.

Conclusion of Complaints

It is the statutory obligation of the DPC to strive to amicably resolve any complaints we receive from members of the public. Throughout 2017, 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 Acts. In 2017, the Commissioner issued 34 decisions of which 30 fully upheld the complaint and four rejected the complaint. A total of 2,594 complaints were concluded in 2017, which is an 80% increase on the 1,438 complaints closed in 2016. *(Case Studies in relation to these complaints are at Appendix II)*

Breakdown of complaints by data protection issue



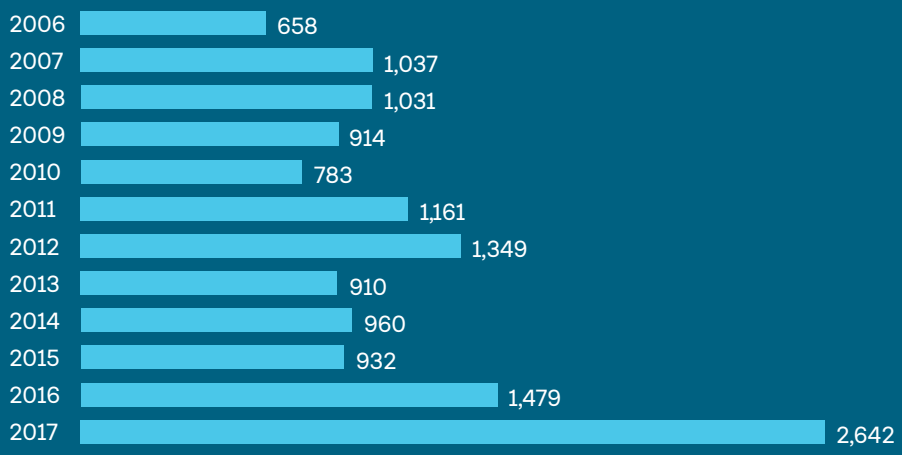
Overview of Complaints 2017

2,642
Complaints received

2,594
Complaints concluded

556
Complaints outstanding at end of year

Number of complaints received since 2006



Right to be forgotten

Complainants concerning the 'Right to be Forgotten' (**RTBF**) or requests for the delisting of internet search results which link to webpages which contain the personal data of the data subject emerged from 2014 onwards following the ruling of the Court of Justice of the EU (CJEU) on 13 May 2014 in the case of *Google Spain v. AEPD and Mario Costeja (C-131/12)* (commonly known as the "Google Spain" decision). The RTBF is based upon Article 12 of Directive 95/46/EC (the Data Protection Directive) which established a right of data subjects to, amongst other things, erasure of personal data or blocking of processing of personal data where the processing does not conform to the rules on processing personal data under the Directive.

Since this CJEU decision, individuals in the EU may, in certain circumstances, request search engine operators to delist internet search results which consist of links to webpages containing the individual's personal data. This right only affects the results obtained from searches made on the basis of a person's name and does not require deletion of the link from the indexes of the search engine altogether. Neither does it provide a right to the data subject for the erasure of their personal data from the third party webpage concerned. The RTBF is not an absolute right and is subject to the data subject establishing that the personal data contained in the webpages to which the search results provide links does not comply with data protection law because it is, for example, irrelevant, excessive, inaccurate, incomplete or out of date.

In the first instance, a request by a data subject for the delisting of a link to a webpage must be made to the search engine operator concerned. However, where a search engine operator refuses to comply with the request, the data subject may complain to their national data protection authority.

In 2017, we investigated 21 complaints concerning the RTBF. Six of these complaints were upheld, 12 were rejected and three are currently under investigation.

CASE STUDY 1: Right to be Forgotten

We received a complaint from a Lithuanian national concerning articles about that individual which had been published by a number of Lithuanian news sources ten years earlier. Links to these articles were returned in search results when a search against the individual's name was carried out using a particular search engine. The articles in question detailed the termination of the individual's employment as an official in a municipal government department in connection with the individual's involvement in potentially fraudulent activities. The article also detailed criminal charges which had been brought against the individual for allegedly accepting bribes in the context of their employment.

During the course of our investigation into this complaint, the search engine operator contended that the information detailed in the articles in question related to serious professional wrongdoing committed by an individual involved in public administration. It maintained that where such wrongdoing resulted in criminal sanctions that this was sufficiently serious for the information to be considered to be in the public interest and therefore any interference with the data subject's rights was justified.

However in the course of our investigation the complainant provided us with official court documents which showed that they had been found not guilty of all the charges which had been referred to in the articles. The complainant also provided us with documents which showed that the termination of their employment with the municipal government department had been on a voluntary basis with the complainant having resigned due to personal reasons. We considered that this documentary information demonstrated that the complainant's personal data, which was being processed by way of the search engine returning search results to the articles in question, was inaccurate, incomplete and out of date and on that basis we requested that the search engine operator delist the links to the webpages in question from search results which were returned from searches conducted against the complainant's name. The search engine operator complied with our request and delisted the links in question.

This case illustrates that the onus is on a search engine, as the data controller, to satisfy itself to the appropriate level that the personal data to which search engine results provide links fully accords with the laws on data protection. In this case, it appeared that the search engine operator did not properly examine the complaint but simply took the approach of assuming that because the complainant had previously been employed in a public official role that the information in question was automatically in the public interest, regardless of whether it was in fact accurate, complete and up to date. The search engine operator had assumed, without apparently even checking the factual background, that the complainant had been convicted of the criminal charges.

Special Investigations

The DPC's Special Investigations Unit 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 special investigations conducted by the Unit during 2017.

Private Investigator Sector

Work continued in 2017 on the ongoing investigation into the Private Investigator sector. Arising from investigations conducted by the Special Investigations Unit, a private investigations company and one of its directors were successfully prosecuted by the DPC in 2017.

Given the high level of breaches which our investigations have uncovered in recent years in this sector, we will continue to focus on this sector for the foreseeable future. If evidence of further behaviour which contravenes data protection law comes to light, further prosecutions will be pursued by the DPC.

CASE STUDY 2: Prosecution of Eamon O'Mordha & Company Limited and one of Its Directors

The investigation of this case arose in the context of a wide-ranging investigation of the Private Investigator sector that commenced in 2016. As part of that investigation, the Special Investigations Unit obtained and examined copies of several private investigator reports written in 2014 and 2015 by Eamon O'Mordha & Company Limited (the company) for its clients in the insurance sector. The Special Investigations Unit became suspicious of the origin of some of the personal data in those reports and it immediately commenced an investigation involving the Department of Social Protection and An Garda Síochána.

The investigation subsequently uncovered access by the company to social welfare records held on databases in the Department of Social Protection. An official in that Department was interviewed by Authorised Officers of the Data Protection Commissioner. During the course of that interview, the official revealed that the two directors of the company were friends of hers and she admitted that one of the company directors met with her regularly and asked her to check information on the Department's database. The official admitted that she carried out those checks and provided personal information to the company director.

Separately, the investigation uncovered access by the company to records held on the PULSE database of An Garda Síochána. Two serving members of An Garda Síochána (who are brothers and nephews of one of the directors of the company) were interviewed by Authorised Officers of the Data Protection Commissioner. During the course of those interviews, both Gardaí confirmed that they had been contacted by their aunt to obtain information from them in relation to individuals and vehicle registration numbers. They both admitted that they had accessed the Garda PULSE database and that they had subsequently passed on personal information to their aunt, the company director.

Eamon O'Mordha & Company Limited was charged with 37 counts of breaches of the Data Protection Acts, 1988 and 2003 (the Acts). All charges related to breaches of section 22 of the Acts for obtaining access to personal data without the prior authority of the data controller by whom the data is kept and disclosing the data to another person. The personal data was kept by the Department of Social Protection and An Garda Síochána. The personal data was disclosed to entities in the insurance sector. Two directors of the company, Eamonn O'Mordha and his wife Ann O'Mordha were separately charged with thirty-seven counts of breaches of section 29 of the Acts for their part in the offences committed by the company. This section of the Acts provides for the prosecution of company directors where an offence by a company is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of the company directors or other officers.

On 8 May, 2017 at Dublin Metropolitan District Court, guilty pleas on behalf of the company were entered to twelve charges for offences under section 22 of the Acts. The Court convicted the company on ten charges and it took the further two charges into account. It imposed ten fines of €1,000 on the company (totalling €10,000). All remaining charges were struck out. Company director Ms. Ann O'Mordha pleaded guilty to twelve charges for offences under section 29 of the Acts. The Court convicted Ms. O'Mordha on ten charges and it took the further two charges into account. It imposed ten fines of €1,000 on Ms. O'Mordha (totalling €10,000). All remaining charges were struck out. The charges against her husband, the other company director, were not proceeded with.

The Hospitals Sector

In 2017 the Special Investigations Unit opened an investigation into the processing of patients' sensitive personal data by hospitals, where such data was being held in publicly accessible areas of hospitals. This investigation 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 (the Acts) to keep personal data safe and secure and to have appropriate measures in place to prevent unauthorised access to or disclosure of personal data.

The investigation involved inspections at twenty hospitals, and included inspections of HSE facilities, private hospitals and voluntary hospitals to give as broad an insight as possible into the processing of sensitive personal data in public areas of hospitals. On a geographic basis, the hospitals inspected represented a broad sample from across the State with eight hospitals inspected in the Dublin area, five hospitals inspected in the greater Leinster region, two hospitals inspected in Connacht, four hospitals inspected in Munster and one hospital inspected in Ulster.

Following each inspection, the Special Investigations Unit drew up an inspection report in respect of the hospital concerned. Each inspection report identified areas of risk that were noted during the inspection and set out recommendations to address the risks identified. The twenty hospitals inspected have each been provided with their inspection report and they have been invited to draw up action plans in relation to the implementation of the respective inspection report's recommendations.

The hospitals inspected during the course of this special investigation were:

- Royal Victoria Eye and Ear Hospital, Dublin
- Mater Misericordiae Hospital, Dublin
- Beaumont Hospital, Dublin
- Our Lady's Children's Hospital, Crumlin, Dublin
- Adelaide & Meath Hospital incorporating the National Children's Hospital (Tallaght), Dublin
- Blackrock Clinic, Blackrock, Co. Dublin
- National Maternity Hospital, Holles Street, Dublin
- St. Vincent's University Hospital, Elm Park, Dublin
- Midlands Regional Hospital, Mullingar, Westmeath

- Aut Even Hospital, Kilkenny
- St. Luke's Hospital, Kilkenny
- Our Lady's Hospital, Navan, Meath
- Wexford General Hospital, Wexford
- Bon Secours Hospital, Cork
- Cork University Hospital, Cork
- University Hospital Kerry
- University Hospital Limerick
- Sligo University Hospital
- University Hospital Galway
- Letterkenny University Hospital

Building on the findings of the twenty hospital inspections, the Special Investigations Unit is currently drawing up an overall investigation report for dissemination in the first half of 2018 to every hospital in the State. This report will bring to the attention of hospitals generally the matters of concern found in the twenty hospitals inspected, including concerns about: controls in medical record libraries; storage of confidential wastepaper within the hospital setting; and lack of privacy when discussing medical and other personal issues. It will also prompt all hospitals to examine whether any or all of those matters of concern are occurring or could occur in their hospital facility and, if so, to implement the recommendations we are making to remedy the situation. Having disseminated the overall report to all hospitals, we will seek an action plan from each of them that outlines how and when they will implement the recommendations that are relevant to their facility. We will monitor the implementation of the action plans over the course of the following twelve to eighteen months.

Tusla (the Child and Family Agency)

In March 2017, the Special Investigations Unit initiated an investigation to examine the governance of personal data concerning child protection cases of the Child and Family Agency (the Agency operates under the name "Tusla").

The establishment of Tusla in January 2014 brought together over four thousand staff across the State who were previously employed within Children and Family Services of the Health Service Executive, the National Educational Welfare Board and the Family Support Agency.

Under its establishing legislation, Tusla was mandated with a number of specific functions which include, but are not limited to, the following:

- to support and promote the development, welfare and protection of children, including the provision of care and protection for children in circumstances where their parents have not been able to, or are unlikely to, provide the care that a child needs;
- to support and encourage the effective functioning of families, to include the provision of preventative family support services aimed at promoting the welfare of children; care and protection for victims of domestic, sexual or gender based violence, whether in the context of the family or otherwise; and
- to provide services relating to the psychological welfare of children and their families.

This special investigation was initiated in response to 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 investigation involved physical inspections carried out by Authorised Officers of the Data Protection Commissioner at Tusla offices at Limerick, Tralee, Kilkenny, Drogheda, Navan, Churchtown, Portlaoise and at the Tusla Head Office in Dublin. Four of the inspections were unannounced.

The Special Investigations Unit completed its investigatory work in December 2017 and its findings (59 in total under twelve topic headings), were presented to Tusla in January 2018.

One of the main conclusions of the investigation was that the processing of personal and sensitive personal data, in the context of file management and record keeping overall was not sufficiently planned for in the form of a robust data governance strategy when Tusla was established in 2014, bringing together a considerable volume of case work and over 4,000 staff from three existing, but distinct, agencies. The following were amongst 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 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 identified, 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 inspection and the findings set out general issues of concern in that regard.

In presenting the findings of its investigation to Tusla, the Special Investigations Unit requested Tusla to present a plan of action within two months outlining how it plans to deal with the findings.

Special Investigation in relation to the Public Services Card

The emergence of what appeared to be a mandatory requirement to produce a Public Services Card (to the apparent exclusion of any other form of evidence of identity) to access a range of non-social welfare services in non-card based transactions triggered a renewed examination of the arrangements for the Public Services Card by the DPC. In addition, articles appeared in the media which drew attention to this matter and the DPC was contacted frequently by members of the public voicing their own concerns. A common theme of concern which arose from members of the public related to data-sharing with other public bodies.

The DPC and the Department of Employment Affairs and Social Protection (the Department) engaged in detailed correspondence in 2017 culminating with the provision to the DPC of the Department's "Comprehensive Guide to Safe Registration and the Public Services Card" and its publication by the Department in October 2017.

Having considered the information provided to her office by the Department, the Commissioner formed the view that further examination was required by her office in order to validate the information received to date from the Department and to assess whether the data controller for the Department is in compliance with his obligations pursuant to the Data Protection Acts, 1988 & 2003. Accordingly, the Commissioner decided to conduct this special investigation using the powers conferred on her pursuant to Section 10(1A) of the Data Protection Acts, 1988 & 2003.

The purpose of this investigation, therefore, is 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 and to evaluate the information that has been made available to the public and whether this meets the transparency requirements of data protection legislation.

The investigation is ongoing with the expectation that findings will be issued to the Department during the first half of 2018.

Data Breach Notifications

In 2017, the DPC received 2,973 data breach notifications under the provisions of the Personal Data Security Breach Code of Practice, of which 178 cases (6%) cases were classified as non-breaches.

A total of 2,795 valid data security breaches were recorded by the office in 2017 representing an increase of just under 26% (571) on the numbers reported in 2016.

From 25 May 2018, Article 33 of the GDPR introduces mandatory data breach notification obligations on organisations. At present, the majority of personal data security breaches reported are submitted under a voluntary Personal Data Security Breach Code of Practice, which was introduced in July 2011. 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 2017. The majority of these unauthorised disclosure breaches occurred in the Financial Sector.

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.

In 2017, the DPC received a total of 178 valid data breach notifications in respect of the Telecommunications Sector, which accounted for just over 6% of total valid cases reported for the year. This represents an increase of 25.3% (36) on the numbers reported in 2016.

Typical examples of data breaches reported to the DPC 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 and paper files; and
- network security compromise/website security breaches e.g. ransomware, hacking, website scraping.

As with 2016, 2017 saw a rise in the number of network security compromises reported with the number of notifications more than doubling from 23 cases reported in 2016 to 49 in 2017. Cases such as these usually include ransomware and malware attacks.

However, there was a decrease in the number of website security breaches reported in 2017, down to 6 from 16 in 2016. These cases typically involve purchasing sites, which hold customer credit card information, whereby attackers focus primarily on scraping credit card details from the site for fraudulent purposes.

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

During 2017, we investigated a number of data breaches involving ransomware attacks. In many instances, we identified a lack of awareness on the part of data controllers that ransomware attacks constitute a breach of the Data Protection legislation. In such attacks, personal data was subject to unauthorised processing and as a result, individuals could potentially be denied the exercise of their rights under the legislation.

We established that where organisations had been attacked by ransomware, the following poor governance and practices were identified:

- a lack of staff training and awareness regarding threats posed by ransomware;
- poorly configured email and web filtering environments or security appliances;
- not ensuring that all computing devices, including servers, were regularly updated with manufacturers' software and security patches;
- poor password policies and a lack of multifactor authentication for remote access;
- poor access controls, specifically the use of shared accounts (roles), and elevated or super user accounts (administrator accounts) on devices without a business need; and
- failure to update antivirus and anti-malware software with the latest definitions.

Data Breach Notifications – 2017

2,973
data breach notifications

6.0% (178)
cases were classified as non breaches — under the provisions of the Personal Data Security Breach Code of Practice.

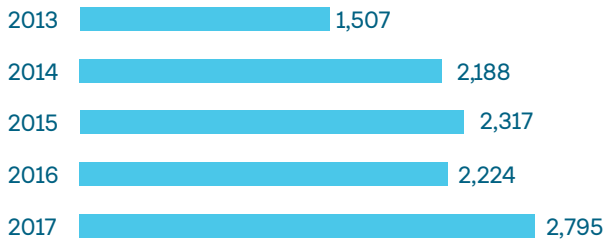
2,795
valid data security breaches recorded by the Office
(01 Jan – 31 Dec 2017)

↑25.7% (571)
increase on the numbers reported in 2016

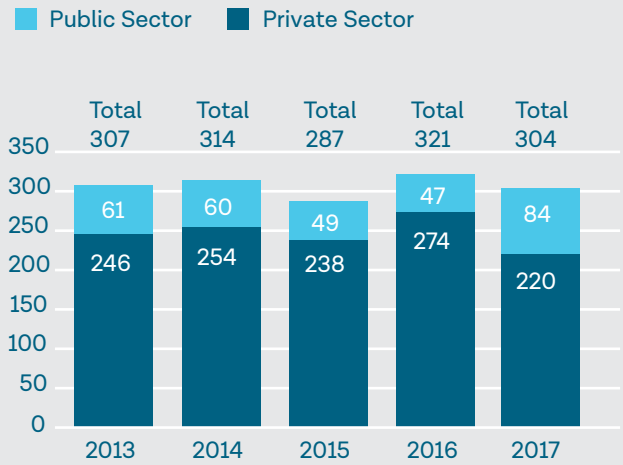
Breach Notifications by Category and Sector 2017

Category	All Sectors	Private Sector	Public Sector
Theft/Loss of IT Equipment e.g. smart device, non-laptop	32	17	15
Website Security	90	24	66
Unauthorised Disclosure — Postal	295	263	32
Unauthorised Disclosure — Electronic	478	341	137
Unauthorised Disclosure — Other	1,844	430	1,414
Security related issues	56	45	11
Non-Breach	178	139	39
Total	**2,973**	**1,259**	**1,714**

Comparison of Breach Notifications 2013–2017



Comparison of Organisations making Breach Notifications 2013–2017



Multinationals and Technology

Supervision of multinational companies with operations in Ireland continued to be a key DPC priority during 2017. Led by the DPC Multinationals and Technology team, we engaged proactively with the multinational sector, ensuring that our regulatory oversight of these companies continued to be coordinated and consistent across the team's advisory, consultation, audit and investigation functions.

Increasingly during 2017, the GDPR featured centrally in our interactions with multinational technology and social network companies, with many companies presenting their GDPR readiness programmes to us and seeking our guidance on the application of the GDPR to their policies, products, and services. These discussions have provided an opportunity to constructively express our views on the implementation of key GDPR provisions such as transparency to service users, the appropriate legal bases for collecting and processing of personal data, and processing of special categories of data. Our engagement with these companies intensified in early 2018 and it is our expectation that our guidance and advice will be instructive in driving GDPR-compliant services and products from 25 May 2018.

2017 also saw a significant increase in enquiries from multinational companies concerning the new GDPR lead data protection authority/one-stop-shop initiative. It is clear from these contacts that a large number of companies with European operations in Ireland are actively assessing if they meet the GDPR requirements to avail of the one-stop-shop model, which will permit them to engage solely with DPC Ireland as their lead EU data protection authority.

In anticipation of being the lead EU authority for many of these companies, work continued in 2017 on preparing the DPC to take on additional functions whereby from 25 May 2018 we will be cooperating more intensively with other EU data protection authorities on cases related to cross-border processing. See section on Page 45 for further information on the DPC GDPR readiness programme.

During 2017, we invested further in building the capacity and capabilities of the Multinationals and Technology team, and in 2018 we will be prioritising further recruitment of specialist resources with expertise in emerging technologies.

Examples of our engagement with multinational companies during 2017, which spanned more than 100 meetings, included:

- consultations with Facebook on many updated and new apps, ensuring our concerns regarding possible personal data processing were taken on board;
- several engagements with LinkedIn Ireland to finalise updates to its privacy policy in 2017, and a similar review of their partner data controller Lynda.com;
- a review of Twitter's current data protection policy;
- engagement with Google on the introduction of a parent controlled account environment for use by children;
- several technology demonstrations and meetings with organisations proposing GDPR products and solutions for data controllers;
- continued engagement with WhatsApp on its transparency regarding data transfers; and
- investigation of several major breaches, including the Yahoo! breach.

High-profile multinational cases

The data protection aspects of a number of high profile commercial developments between large technology multinationals were the focus of close scrutiny by the Multinational and Technology team during 2017. These included the proposed sharing of WhatsApp user data with Facebook, the takeover and reorganisation of the Yahoo! EMEA operations by the Verizon group forming the new "Oath" Data Controller, and the outcome of the Microsoft takeover of LinkedIn.

WhatsApp — Facebook

Extensive engagement with WhatsApp continued on the legal basis and on fair processing of any personal data that is shared or transferred from WhatsApp to Facebook. This resulted in the positive and corrective change to transparency levels for users when a revised FAQ with improved details on the nature, scope and purposes of the data sharing was published by WhatsApp in August 2017. At the same time, the agreement and commitment made by WhatsApp to DPC Ireland in 2016 that resulted in a pause on data sharing for purposes other than security and performance analytics processing remains in place. Importantly, sharing for the purposes of advertising on Facebook or product improvements for Facebook or WhatsApp remains on hold. This specific data sharing will not now take place until an agreed mechanism to enable it is put in place, to the satisfaction of the DPC.

Oath EMEA — Yahoo!, Verizon Group

In June 2017, the Verizon Group completed its acquisition of Yahoo! In Ireland, the main establishment and data controller for Yahoo! members in Europe. Yahoo! EMEA, has now become Oath EMEA, part of the Oath digital media business. As a global organisation with more than 50 brands and millions of users in the EU, it has been important for Oath EMEA to engage with the DPC so that we can understand the impact of the acquisition and re-organisation. A significant element of this engagement has been the consideration of the changed or new data sharing arrangements and responsibilities that Oath EMEA as data controller and data "exporter" undertakes and is accountable for. The DPC engaged with Oath EMEA on this matter and continues to monitor progress on foot of recommendations already made. We are also continuing to engage with Oath EMEA on their GDPR readiness programme.

Microsoft — LinkedIn

In December 2016, Microsoft completed its acquisition of LinkedIn. In 2017, LinkedIn confirmed to the DPC that Microsoft and LinkedIn remain separate and independent data controllers. We continue to engage with LinkedIn on how this situation will develop in terms of any data sharing that may occur in the future, in particular around the legal basis, transparency and safeguards that are in place.

Engagement with Facebook Ireland

The DPC engaged with Facebook throughout 2017 on a range of matters including transparency to users, controls and safeguards for users related to a variety of new apps involved in the processing of photos, location and text messaging. We reviewed updated terms, new terms and policies about the matters involved, undertook detailed examinations of the technology being used in the collection and processing of personal data and provided extensive feedback and observations. While much of the DPC guidance was made in the context of Facebook's preparation for the GDPR, Facebook agreed to accept our recommendations when apps and services were being released for Irish and EU audiences prior to the GDPR. Through our intensive engagement with Facebook we have been able to better understand Facebook's intended processing operations and to drive better compliance.

In addition to changes in language in policy documents and updates to the cookie statement, there were a number of interesting topics during consultation that warranted further exploration with Facebook.

LiveLocation in Messenger

The use of location data by apps and websites is increasingly common as a means to make personalised suggestions and recommendations based on physical world buildings, shops, facilities, products, services or people that are nearby. For some individuals this proves very useful in certain situations. However, its collection, processing and sharing with data controllers comes with some risks. The information can be very revealing about a person's physical location or habits and it requires special care and attention when it is collected, processed or made available to others.

It was in this context that we engaged with Facebook during 2017 on an update to their Messenger product called "Live Location". This allows individuals to choose to share their location with others in a conversation for a set period of time. We were concerned in particular about the transparency and retention of location data collected by this feature and raised various technical questions regarding the means and "application programming interfaces" that have been used to obtain and process location information regarding the user.

We confirmed in this process that the location data sharing is at the control and choice of the user, that the location data is not retained by Facebook — and so is not available in their Download Your Information tool — and that device level APIs and controls are used to collect the information by the app at all times. On foot of this engagement we provided Facebook with observations and recommendations regarding the continuous collection of location data by the Messenger app. We provided further recommendations on the availability, consistency and granularity of location controls for Facebook users, and emphasised that further substantive updates to the collection and processing of location data by Facebook would be discussed with the DPC if and when they arise.

Engagement with LinkedIn Ireland

LinkedIn Salary Reporting

LinkedIn proposed to roll out its Salary Reporting website feature in various jurisdictions outside the USA, and including on some EU locations. The feature allows a data subject to enter their salary information for a position they hold in exchange for an aggregate indication of salary levels in the same role, industry or broad location. The information is de-identified, encrypted, access-controlled and not stored in association with a member's profile. A quorum of submitted salaries must be submitted before aggregate information is made available to avoid any relinking or singling out possibilities. Our engagement focussed on exploring the safeguards that were in place to protect this sensitive information, its availability internally and the associated data processing. LinkedIn have published information regarding this feature on its engineering blog. We continue to monitor in order to ensure that the consent basis for the data processing, the safeguards and risk management that are in place remain of high quality and ensure that where this feature is in place in 2018 that it is GDPR compliant.

LinkedIn Offsite Collection ("Profile Suggestions")

Another feature put in place by LinkedIn during 2017 was their collection of information made available on a limited set of websites where individuals may have published or made "publicly available". Where LinkedIn collected this data it would confirm with a member whom it had algorithmically identified that the information related to them. If so, the member can choose to add it to their LinkedIn profile. Our concerns centred on the transparency and the controls available to LinkedIn members, and possibly non-members, whose personal data LinkedIn were collecting. It became clear when we explored this feature with LinkedIn that it was consent-based, and that members could choose to prevent the processing enabling this feature from taking place. In addition, where public data was collected but not positively identified LinkedIn identified that it was retained for a very limited time period. We have made clear to LinkedIn that our observations and recommendations concerning this feature be carefully managed, particularly in terms of transparency, controls and risk mitigation regarding the non-member personal data processing.

Engagement with Twitter

Twitter Location Data Collection

During a review of a proposed update to Twitter's privacy policy and related processing operations, the team decided to look more closely at the collection and use of location data. This was of particular interest because, as already noted in relation to Facebook services above, the sensitivity of location data can reveal intimate details about an individual. In this case, while Twitter obtain opt-in consent for the collection and use of location data from terminal equipment used to access the service, location data may also be collected from home router equipment even where consent is not given. For Twitter users who wish to "Tweet with Location" this may allow them to label their tweet with a specific business, landmark, or point of interest.

In exploring this processing operation by Twitter we analysed both their technical and organisational safeguards, the necessity for this processing and the legal basis. In particular, we recommended to Twitter that they revisit the legal basis for processing of location data from account-holder or third-party router equipment in order to fully consider and be able to demonstrate their accountability, necessity and balance of processing with data subject rights and freedoms. We also recommended that Twitter consider again their provision of adequate and easily-used safeguards and opt-out controls, and the accessibility and availability of documentation to allow users to provide fully informed and precise consent for all means of location data processing. Twitter confirmed that their response to our recommendation would be progressed as part of their GDPR readiness work.

Multinational companies and data breaches

In 2017, the Multinationals and Technology team investigated 19 data breaches which involved multinational organisations. We found the majority of these data breaches involved:

- an overreliance on data processors to implement appropriate security measures relating to personal data processing, such as reliance on the default security settings offered by cloud-based providers, which in many cases led to unauthorised access to personal data;
- a lack of awareness of security features provided by software and hardware ICT solutions used for personal data processing, for example, those provided by operating systems, software applications, cloud-based providers etc., and a failure to review and implement those features as appropriate;
- failure to undertake periodic reviews of security measures, the configuration of those security measures, and failure to apply critical updates and security patches;
- failure to have appropriate data processing agreements in place, leading to poor governance and controls regarding data processors and failure to ensure that data processors complied with their obligations to securely process personal data on the instruction of the data controller; and
- overreliance on data processors regarding the determination and implementation of appropriate security measures to protect an organisation's personal data processing. We established that organisations did not seek formal assurances from their data processors that the security controls implemented were appropriate and met the organisation's specific security requirements to protect the processing of personal data.

Yahoo! data breach

Following notification to the DPC by Yahoo! EMEA and Yahoo! Inc. of a data breach in September 2016 whereby approximately 500 million Yahoo! user accounts had been copied and stolen from Yahoo! Inc. infrastructure in 2014, we initiated an investigation under Section 10 of the Data Protection Acts 1988 and 2003. Yahoo! EMEA is the data controller for the subset of accounts associated with EU/EEA citizens, and Yahoo! Inc. the data processor.

Our investigation was largely concluded in 2017 and will be finalised in early 2018.

Data Protection audits of Multinational companies

During 2017, the Multinationals and Technology team conducted data protection audits of a number of multi-nationals including:

- Adobe Systems Ireland;
- LinkedIn Ireland Limited;
- SurveyMonkey; and
- AIG.

The key findings that emerged from these audits included:

- a lack of transparency due to privacy policies that do not adequately inform data subjects as to the processing of their personal data;
- no defined data retention policy as required under Section 2(1)(c)(iv) of the Data Protection Acts 1988 and 2003 leading to data being retained for indefinite periods;
- overreliance on data processing contracts as a means of compliance. In many instances, we identified that organisations were not taking appropriate steps to verify that personal data they hold was secure and processed on the specific instructions of the data controller; and
- overreliance on global organisational security policies. We identified that some organisations were reliant on global security policies, which did not meet the specific needs of organisations acting as data controllers in Ireland. We also identified in some instances that organisations had little or no input into the development of these security polices, leading to poor ICT governance and the implementation of security measures that were inadequate to meet their obligations under the Acts.

Cooperation with European Data Protection Authoraties

The Multinationals and Technology team received 19 co-operation requests or referrals of cases from a number of European Data Protection Authorities (DPAs) in 2017.

In one instance, we assisted the Dutch DPA with regard to data processing by Airbnb Ireland ("Airbnb") of Dutch National Identity Numbers ("BSN"). Airbnb is a data controller established in Ireland with responsibility for all of the company's European users. In the Netherlands, users when verifying their identity on Airbnb had the possibility of uploading a digital copy of their passport or a similar document. These documents can contain an individual's BSN, which is a unique identifier classified as a so-called 'special category' of personal data in the Netherlands. The processing of special categories of data is prohibited in the Netherlands, unless a specific legal exception applies.

Following an investigation by the Dutch DPA and with assistance from the DPC, Airbnb Ireland ended the processing of the BSN. Airbnb deleted all previously collected BSNs and implemented controls and processes to ensure the immediate and automatic deletion of BSN data from all digital copies of Dutch identity documents uploaded to its platform.

This case is an example of effective cooperation between EU data protection authorities that the GDPR aims to streamline and strengthen.

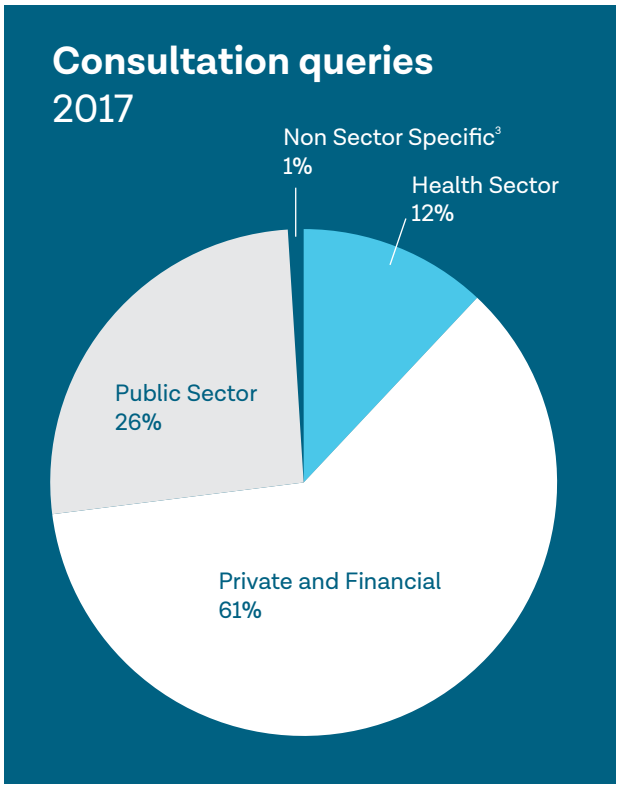
Consultation

The consultation function plays a pivotal role in advancing a better understanding and awareness among organisations of their data protection obligations. Through active and meaningful engagement with both public and private sector organisations we ensure that data controllers and processors are responsible and compliant with data protection legislation and that protection of this fundamental right is at the forefront of any project involving the processing of personal data. Taking a strategic approach to our engagement with organisations, in 2017 we continued to focus on proposed data processing projects and initiatives that posed a high risk to the data protection rights of individuals. By providing clear guidance and advice to organisations on their compliance obligations, the DPC's proactive consultation work continued to deliver results in protecting the public from poor data handling practices by both public and private sector bodies.

2017 General Queries

General consultation queries increased significantly in 2017 to a total of 1,818 queries. This represents an increase of 69% from 2016's 1,078 queries and an increase of 111% compared with 2015. Note: these figures do not include consultations with multinational companies, details on which are included on Page 26.

In contrast to 2015 and 2016, the consultation queries were not as evenly divided amongst the various sectors, with a notable increase in 2017 of general queries from the private sector and, in particular, from small to medium size businesses:



The breakdown of the general consultation queries is very informative and it was apparent that almost every query received in 2017 involved, either directly or indirectly, consideration of the impending GDPR. The level and the nature of the queries would indicate that data protection is becoming a more significant boardroom issue with many organisations now actively preparing for the GDPR. It is clear and welcome that there is a growing appreciation among data controllers and data

[3] Does not include multinationals and technology issues

processors of the importance of data protection and the reputational damage and financial loss that can be caused by the mishandling of personal data.

Another very noticeable trend in 2017 was the increase in the volume of queries received from data protection consultancies and law firms seeking input from the DPC on how to advise their clients on particular data processing issues concerning the GDPR. That many organisations are seeking relevant expertise to assist them in getting prepared for the GDPR is to be welcomed and the DPC will continue to provide guidance and advice, as appropriate. In this context, it is imperative to note however, that in line with the principle of accountability, it is a matter for the organisations involved and their advisors to be able to stand over and justify their data processing arrangements and to be able to demonstrate compliance with the GDPR.

It is expected that the growth trends experienced by the consultation unit will continue for 2018 given the increasing level of awareness of individuals of their data protection rights as well as a growing acknowledgment by organisations that compliance with data protection is a key component to the successful delivery of projects/ventures which involve the processing of personal data. The implications of the GDPR are becoming very clear and very real to many organisations and the consultation unit will continue to raise awareness throughout 2018 to assist those organisations in preparing for and implementing the GDPR.

Engagement

The consultation section proactively engaged with a wide range of stakeholders, providing the appropriate direction and guidance allowing data controllers to confidently make decisions about projects/proposals involving personal data. Over 100 face-to-face meetings were conducted during the year.[4] Some of the organisations/groups and projects (exploratory or otherwise) that we engaged with during 2017 included the following:

Public Sector

- Department of Social Protection — Public Services Card
- Department of Agriculture — GDPR readiness plan
- Department of Communications Climate Action and Environment — Television Licence
- Central Statistics Office — Mobile Phone Data and Tourism Statistics
- Department of Housing — Online Planning Submissions
- An Garda Síochána — Community CCTV and input into Data Protection Impact Assessment Templates
- National Archives Office — the National Archives Act and implications under the GDPR
- Department of Public Expenditure and Reform — Data Sharing and Governance Bill, eCohesion IT System, the Hive platform, Civil Service Shared Learning and Development Service
- Department of Finance and Companies Registration Office — Beneficial Ownership Register
- Taxi Regulator — CCTV use in Taxis
- Department of Children and Youth Affairs — Reform of the Guardian ad Litem Service
- Charities Regulator — Input into GDPR guidance
- HEAnet — GDPR service checks for the Higher Education Sector
- Irish Aviation Authority — Impact of Drones on Privacy and Data Protection
- European Space Agency

[4] Does not included meetings with multinational companies. See section on 'Multinationals and Technology' for further details

- Department of Justice and Equality Working Group on Insurance fraud
- Revenue Commissioners update on FATCA & CRS automatic exchange of Tax information and GDPR readiness

Health Sector

- HIQA — National Patient Experience Survey & Input into Data Protection Impact Assessments Guidelines
- RCSI — GDPR preparedness
- Medtronic, Novartis, Irish Pharmaceutical Health care Association — GDPR and implications for the Pharmaceutical Industry and Clinical Trials.
- Department of Health — Newborn Screening Cards and retention of health data.
- Department of Health, the HSE and HIQA — Health Information Policy Framework
- Genetics Medicines Ireland — Processing of health data for research purposes
- BBPRM draft Code of Conduct
- Nursing Homes Ireland and GDPR Readiness

Charity Sector

- The Wheel — GDPR readiness
- Charities Institute of Ireland — GDPR readiness
- Pavee Point — GDPR readiness

Private/Financial Sector (excluding multinational sector)

- AIB — GDPR preparedness
- Toy Industries of Europe — GDPR preparedness
- Health and Safety Review — Sectoral Impact of GDPR
- Banking and Payment Federation of Ireland — PSD2
- Marketing Network — GDPR readiness
- Insurance Ireland meeting with compliance officers
- Irish League of Credit Unions
- Irish Credit Bureau
- Central Bank of Ireland — AML compliance
- Moodle — GDPR readiness
- Deloitte — GDPR readiness
- World-check / Thomson Reuters — GDPR readiness
- Davys — GDPR readiness
- Aviva — Insurance fraud
- Virgin Media — GDPR readiness

Legislative Observations

Comprehensive observations on draft legislation were also made to various government Departments during 2017. Examples included:

1. General Scheme of a Bill to provide for the Central Bank to establish a National Claims Information Database
2. Affordable Childcare Scheme — The Childcare Support Bill
3. Data Protection Bill
4. Data Sharing and Governance Bill
5. Vehicle Registration Data (Automated Searching and Exchange) Bill 2017
6. Amendments to the Taxes and Consolidation Act 1997

In 2018, formal consultation mechanisms provided for by the GDPR and the Data Protection Bill will be implemented. These include mandatory consultation under Article 35 (Data Protection Impact Assessments), and 36 (Prior consultation with Public Authorities), and approval of Codes of Conduct.

Examples of proactive sectoral engagement

Local Authorities in Ireland play a hugely important role in the lives of citizens, including in the provision of a wide range of primary services, the management of public infrastructure, law enforcement, and the promotion of social inclusion and cohesion. In carrying out all of their functions Local Authorities collect, hold and process the personal data of individuals on a uniquely large scale and for a great many purposes. As data controllers, Local Authorities rank as some of the largest in the state including both public and private sectors, and hold portfolios of personal data covering a large array of categories. In 2017, the DPC commenced work on developing sector-specific and practical guidance for Local Authorities in relation to data protection best practice and to assist those organisations in complying with the GDPR. This guidance will be finalised in early 2018.

It is also the intention to provide similar sector-specific guidance to other areas such as the **charity** and **health research** sectors during 2018.

One of the significant areas of development that emerged in 2017 in the **Financial Sector** was the entry into the marketplace of third party payment and account information service providers under the Payment Services Directive EU 2015/2366, 'PSD2'. In 2018, we will continue, and expand upon, engagement commenced in 2017 with key stakeholders including industry representative bodies, financial services regulators, relevant Government Departments, and our European counterparts and colleagues to assist both banks and new entrants from the FinTech sector in ensuring that the processing of personal data in the provision of innovative payment products under PSD2 is compliant with data protection law. In particular, the key GDPR principle of transparency must be adhered to in a rapidly changing digital environment where customers may not always be aware of the full data protection implications of making use of new products and services.

We will also continue to engage with the Financial Sector in relation to other, evolving, regulatory areas such as anti-money laundering (in relation to the 4th and anticipated 5th EU Anti Money Laundering Directives), anti-fraud and credit reporting which involve the large scale processing of customers' personal data. The ongoing development of online and connected financial services is closely connected to the growth of big data analytics and customer profiling within the industry and this will also be a focus of engagement with industry in 2018, in collaboration with our colleagues at a European level.

Data Protection Audits

In 2017, 91 audits/inspections were carried out in total (the list of organisations audited is at Appendix 1). The aim of all audits and 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. 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.

In terms of audits conducted in 2017, our target selection was 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. Audits may also be supplementary to investigations carried out by the DPC in response to specific complaints or allegations received and in 2017 this led to a series of audits of accommodation centres operating under the direct provision system. Audits were also conducted in the retail sector in tandem with the GPEN Privacy Sweep and a key outcome of this series of audits was the publication of guidance regarding e-receipts. Another key focus was the supervisory duties assigned to the DPC under legislation such as the Communications (Retention of Data) Act 2011, culminating in a series of audits of Communication Service Providers (Three, Virgin Media, BT Ireland)(CSPs).

In 2017, in terms of the public sector we conducted audits of the Irish Prison Service's *Prisoner Information Management System*, government schemes such as the Department of Employment Affairs & Social Protection's *JobPath Employment Activation Programme* (Seetec, Turas Nua), the Department of Agriculture's *Knowledge Transfer Scheme* and the *HSE's National Medical Cards Unit*. Also selected for closer examination was the deployment of the Sierra library management system nationwide through an audit of Malahide Library. At the end of 2017, we commenced our supervision of the newly established Central Credit Register, established by the Credit Reporting Act 2013, with an inspection of the system, pre-data population.

Audits of private sector entities included Irish Life Health, AIG, Gohop and Survey Monkey as well as transport companies, hotels and a number of letting agents. Cognisant that the remit of the DPC also extends to the voluntary sector, we conducted audits of Threshold, Sonas, Barnardos, Foster Care Ireland and Family Care Association in 2017.

Accommodation Centres

In 2017 we received an allegation concerning the alleged misuse of CCTV in an accommodation centre for asylum seekers, specifically, in relation to remote access by staff to live CCTV footage via a smartphone. In addition, inappropriate video recording of residents by staff using their personal smartphones was alleged.

In line with our powers designated under Section 24 of the Data Protection Acts, we conducted unannounced inspections of St Patrick's Accommodation Centre, Monaghan and Mosney and Athlone Accommodation Centres. We determined there was no evidence of any breach of the Data Protection Acts with regard to any of the allegations.

From the outset, we engaged with the Reception & Integration Agency (RIA) to ensure that a generic CCTV policy would be drawn up by RIA and issued to all accommodation centres. We noted the finalised CCTV Policy confines the use of CCTV to a narrow set of purposes namely the security, health, and safety of both residents and staff and the explicit restriction placed on smartphone/remote access to CCTV footage except in emergencies. In terms of transparency, the inclusion of a notice regarding CCTV in the letter of acceptance signed by all residents prior to taking up residence is to be welcomed, as is the commitment to incorporate CCTV and data protection into the inspections of accommodation centres which are published on the RIA website.

We will continue to monitor this area closely and have issued general advice to a wide range of entities audited in 2017 concerning the inappropriate use of CCTV to monitor individuals either on-site or remotely.

Malahide Library and the Sierra Library Management System

The background to the inspection of Malahide Library stems from an engagement the DPC had with the Libraries Development Unit in the Local Government Management Agency (LGMA) in 2015 regarding the rollout of a single library management system (Sierra) for all public libraries in Ireland. During the course of this engagement, the DPC outlined that it considered there were potential issues surrounding consent and inappropriate access; that access controls and trigger mechanisms would need to be considered and that a built-in audit trail functionality (both read and edit access) would be expected in the finalised version of the Sierra. At the time of the engagement, the DPC singled out the Sierra project for future examination via an audit once Sierra was live across the majority of libraries in Ireland. Malahide Library was subsequently selected for audit.

Shortly before the August 2017 audit of Malahide library, Fingal County Council contacted the DPC informing it of a recent incident where a library staff member based in another local authority inadvertently came across the borrower record of a library borrower in Fingal which contained data entries of a highly inappropriate, sexually explicit nature. Fingal County Council established subsequently that the records of 20 Fingal library borrowers had been edited in this manner and these records had in fact been imported from the previous library management system Galaxy onto Sierra.

The DPC established that there was no audit trail functionality in relation to the amendment of borrower records on either the Galaxy or Sierra systems that would assist in identifying the source of the edits. In addition, it was noted that library staff login to Sierra with generic logins for each library.

The DPC subsequently instructed the Libraries Development Unit in the LGMA to take the following measures:

- Audit Trail functionality should be implemented as a matter of priority facilitating the generation of logs for all look ups and edits on Sierra;
- individual unique logon usernames and passwords should be assigned to every individual user accessing the Sierra National Library Management system; and
- functionality should be built into Sierra where staff are automatically prompted to change their passwords on a regular basis.

The GDPR imposes a legal requirement on all data controllers to notify the DPC of a breach. Article 4(12) of the GDPR defines a personal data breach as a

> "breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

Thus, under the GDPR both the unauthorised access to, or alteration of, the borrower record in the manner outlined will constitute a notifiable data breach.

E-receipts / GPEN Sweep

In 2017, the Global Privacy Enforcement Network conducted its 5th annual Privacy Sweep. The investigation was undertaken by 24 data protection regulators from around the world, including the DPC.

The privacy notices, communications and practices of 455 websites and apps in sectors including retail, finance and banking, travel, social media, gaming/gambling, education and health were assessed to consider whether it was clear from a user's perspective exactly what information was collected, for what purpose, and how it would be processed, used and shared.

The Irish Sweep focussed on two specific areas; the use of e-receipts by retail companies and on Multinational and Irish based companies offering online travel services in Ireland.

The Sweep found that in 94% of cases, retailers offering e-receipts to customers provided no information on their websites with regard to the processing or deletion of email addresses gathered for this purpose.

In the case of online travel organisations, the sweep focused on how these organisations obtain and process personal data online, their communication with users on their data processing operations and the ease with which users can exercise their rights in the course of using online travel services in Ireland. The sweep established a general lack of transparency towards individuals regarding the processing of their personal data and we specifically found that:

- privacy communications across the various sectors tended to be vague, lacked specific detail and often contained generic clauses;
- the majority of organisations failed to inform the user what would happen to their information once it had been provided;

- organisations were generally quite clear on what information they would collect from the user;
- organisations generally failed to specify with whom data would be shared;
- many organisations failed to refer to the security of the data collected and held — it was often unclear in which country data was stored or whether any safeguards were in place; and
- just over half the organisations examined made reference to how users could access the personal data held about them.

In conjunction with the Sweep, the DPC carried out a series of audits in order to assess how organisations gather and process personal data in the course of providing e-receipts to customers. In a number of cases we found evidence of email addresses, gathered for the purpose of issuing e-receipts, being used to subsequently issue marketing material. Following these audits, we published guidance around the use of e-receipts which highlights the potential penalties involved where non-compliance is found.

Communication Service Providers

The Communications (Retention of Data) Act 2011 transposed the Data Retention Directive (2006/24/EC) placing requirements on certain communication service providers (telecommunications companies and providers of publically available electronic communications services) to retain call traffic data (not content). Phone and mobile traffic data are required to be retained for two years; internet communications for one year.

As per provisions contained in the Communications (Retention of Data) Act 2011, disclosure requests are made to communication service providers (CSPs) by An Garda Síochána, the Defence Forces, the Revenue Commissioners, the Garda Síochána Ombudsman Commission and the Competition and Consumer Protection Commission. Having conducted audits of these prescribed state agencies, we commenced a series of audits of disclosure requests processed by CSPs beginning with eir and Meteor in Q4 2016 and continued with this programme of audits in 2017, auditing Three, Virgin Media and BT Ireland.

The DPC's oversight role is to ensure that the processing of disclosure requests by CSPs is done in compliance with the Data Protection Acts 1988 & 2003. In addition, section 4(2) of the Communications (Retention of Data) Act 2011 — ***Data Security*** — assigns a specific role to the DPC — "The Data Protection Commissioner is hereby designated as the national supervisory authority for the purposes of this Act and Directive No. 2006/24/EC of the European Parliament and of the Council."

General Findings & Recommendations

In terms of CSPs fulfilling disclosure requests, it is important to note that Section 7 of the Communications (Retention of Data) Act 2011 (CRDA) legislates that provision of the data by a CSP is mandatory — "A service provider shall comply with a disclosure request made to the service provider." Hence this series of audits focused on data security and the procedures and systems for processing disclosure requests within the CSPs.

In terms of the technical security and organisational measures the key recommendations were as follows:

- CSPs should ensure that where processing of personal data is carried out by a Data Processor to support its CDRA requirements on behalf of a CSP, the CSP should ensure that the processing is carried out in pursuance of a contract in writing or in another equivalent form between the CSP and the Data Processor;
- the contracts should include that the Data Processor carries out the processing only on and subject to the instructions of the CSP and that the Data Processor complies with obligations equivalent to those imposed on the Data Controller by section 2(1) (d) of the Acts. The contract should include at a minimum the following:
  - » instructions as to what the Data Processor can do with the personal data provided and processed including the conditions under which the data may be processed;
  - » detail security measures for the personal data to protect it from damage, theft, accidental loss and unauthorised access;
  - » the right to audit the Data Processor to ensure compliance with the provisions of the contract; and
  - » obligations to delete or return data on completion or termination of the contract;
- CSPs should implement contract monitoring processes to ensure that Data Processors are compliant with the contract terms;

- CSPs should define and implement documented processes for role-based user access to systems supporting the CDRA. These reviews should be carried out at appropriate risk based intervals, and should include users, administrators, third party and system/service accounts;
- CSPs should ensure that users' access roles are reviewed and signed off by appropriate management level. User accounts that are no longer required, such as staff which have left the organisation or moved within the organisation should be disabled or removed;
- CSPs should conduct specific ICT risk assessments regarding the systems supporting the CDRA. Such assessments should be conducted at regular intervals and consider the likelihood and potential impact to a system supporting the CRDA; and
- CSPs should ensure appropriate safeguards are in place to mitigate and protect against an evolving threat landscape such as, intrusion prevention and detection, strong authentication, ongoing staff training and awareness and advanced malware protection.

In terms of procedures and oversight within the CSPs, the majority of the recommendations issued were best practice in nature and included the following:

- all disclosure requests made to CSPs in relation to subscriber requests should be recorded and filed according to the specific legislation cited in relation to each request; and
- other recommendations focused on internal audit, governance arrangements, the need for procedural documentation, transparency and retention policies.

The DPC will conclude its series of audits of CSPs in 2018 and notes the draft legislation announced by the Department of Justice & Equality in July 2017 (Retention of Data) Bill 2017 and the findings of Mr Justice John L Murray's April 2017 report — 'Review of the Law on the Retention of and Access to Communications Data'.

Audit Findings

Themes identified in the 2017 audits include the following:

1. Security of personal data

Personal data, whether in manual or electronic format, should be kept safe and secure. Some of the issues identified during our audits are as follows:

- no audit trails of systems in place;
- no access controls implemented by organisations to limit access to personal data only to those employees with a business reason to access it;
- no prompts on systems to alert employees to change their password;
- use of generic usernames and passwords;
- ad hoc arrangements for the shredding of confidential waste; and
- ad hoc arrangements for storing and archiving of physical records.

2. Monitoring of systems to identify inappropriate access

Most systems now contain audit trail functionality which records a log of amendments or edits made within a database or system. However, a log of any 'look-ups' on a system by employees should also be recorded. 'Look-ups' on systems can occur when an employee may search for a particular record to view information but not make any amendments to that record. The deployment of audit trail functionality to identify whether a record has been viewed or amended is core to overseeing the appropriate use of personal data by an organisation's employees. In addition, a proactive monitoring programme to detect recent or ongoing inappropriate access or unusual access patterns is another vital safeguard. Employees should also be made aware of the importance of only accessing personal data for legitimate business reasons and of the fact that such audit trail functionality is in operation.

3. Retention Policies

Under Section 2(1)(c)(iv) of the Data Protection Acts, data "shall not be kept for longer than is necessary for that purpose or purposes". The implementation of retention periods by organisations together with maintaining a retention schedule of the different categories of personal data are effective tools for ensuring personal data which is no longer necessary is regularly deleted. Personal data should not be kept in scenarios where an organisation believes that there 'may' be a use for it at a later stage.

4. CCTV

Inappropriate use

Organisations usually deploy CCTV for security purposes which can be deemed to be justifiable and proportionate in scenarios of ongoing theft. However, other uses of CCTV would also need to be justified and proportionate. For example, continuous monitoring of employees for performance issues would likely fail the proportionality test. CCTV should not be used as an alternative to the effective supervision of employees, either on-site or remotely. Remote access to CCTV footage via smartphones, tablets etc. is becoming more commonplace and is clearly advantageous in situations such as monitoring an empty building. However, there would need to be a very high level of justification required for remotely monitoring employees during the course of carrying out their normal daily working duties.

Requests for Access to CCTV by An Garda Síochána

Requests for copies of CCTV footage by An Garda Síochána should only be acceded to where a formal written (or fax) request is provided to the data controller stating that An Garda Síochána is investigating a criminal matter. For practical purposes, and to expedite a request speedily, a verbal request may be sufficient to allow for the release of the footage sought. However, any such verbal request must be followed up with a formal written request. It is important for data controllers to maintain a disclosures log of all Garda requests.

In general terms, a request from An Garda Síochána to simply view CCTV footage on the premises of a data controller or data processor would not give rise to specific concerns from a data protection perspective.

5. Electronic Marketing

As highlighted in previous annual reports, the marketing operations of organisations were again examined during this year's audit programme. Obtaining valid consent from individuals to send them marketing communications is a vital step for organisations in adhering to the marketing regulations (Regulation 13 of S.I. 336 of 2011). Phone numbers and email addresses which were collected for other purposes such as delivery or warranty purposes, or for providing a customer with an e-receipt cannot be used subsequently for marketing purposes without the consent of the individual. Under S.I. 336 of 2011, the onus is on the marketer to prove that it had valid consent of the individual to send them electronic marketing communications. Summary proceedings for an offence under this regulation can be brought and prosecuted by the Commissioner.

6. Deletion of Vetting Information

Many organisations are required to have prospective employees vetted if they are seeking to work with children or vulnerable adults. eVetting has been introduced by An Garda Síochána in an attempt to reduce processing times. The eVetting process has determined that a prospective employee is required to submit proof of identity with their application to the relevant organisation. It has placed the onus on the organisation to validate proof of identity of the prospective employee. Data submitted as part of the vetting application, such as identity documentation together with the vetting disclosure document issued by An Garda Síochána to the relevant organisation, should be routinely deleted one year after they are received except in exceptional circumstances.

In response to findings such as these, our teams make best-practice recommendations and provide immediate direction to an organisation to take a particular action.

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

Legal

Data protection proceedings involving the Commissioner

The Commissioner was party to a number of proceedings before the Irish Courts in which judgment was delivered during 2017. These cases are summarised below.

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 must be followed by an EU data protection authority where a complaint is made by a data subject which concerns an EU instrument, such as an EU Commission decision.

(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 Maximilian Schrems concerning the transfer of personal data by Facebook Ireland to its parent company, Facebook Inc., in the US. Mr Schrems was concerned that, because his personal data was being transferred from Facebook Ireland to Facebook Inc., his personal data was then being accessed (or was at risk of being accessed) unlawfully by US state security agencies. Mr Schrems' concerns arose in light of the disclosures by Edward Snowden regarding certain programmes said to be operated by the US National Security Agency, most notably a programme called "PRISM". The (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 the basis that 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 its judgment, the High Court decided that the concerns expressed by the Commissioner in her draft decision of 24 May 2016 (referred to above) 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.

(6) Questions to be referred to the CJEU

Following the delivery of its judgment, the High Court convened a series of further hearings. The primary purpose of these hearings was to enable all of the parties, including the amici, to make submissions to the Court as to the precise formulation of (i) the questions to be referred by the High Court to the CJEU and (ii) the particular findings of fact to be presented by the High Court to the CJEU against which the CJEU will in turn be asked to answer the relevant questions of EU law. These hearings took place on 1 December 2017, and 17 — 19 January 2018 with the Court reserving its decision as to the referral questions. At the time of going to print there is no indication as to when the Court will deliver its decision in respect of the precise questions which it has decided to refer to the CJEU and the other issues raised during the course of the hearings in December 2017 and January 2018.

(7) Materials relating to the case

The judgment and executive summary of 3 October 2017, together with interim judgments on procedural matters in these proceedings, have been published on the Commissioner's website. Transcripts of the substantive hearing before the High Court and the expert witness reports provided on behalf of the Commissioner are also available on the Commissioner's website.

An appeal to the High Court in the case of *Shatter v Data Protection Commissioner* [2017] IEHC 670 (Judgment delivered on 9 November 2017 by Meenan J.)

This appeal originated with a complaint made to the (then) Data Protection Commissioner against the appellant, Mr Shatter, by a data subject, Mr Mick Wallace, T.D., concerning certain matters disclosed by Mr Shatter about Mr Wallace during a debate on RTÉ's Prime Time programme in May 2013. During that debate, Mr Shatter had alleged that Mr Wallace had been cautioned by An Garda Síochána for using a mobile phone while driving. Mr Shatter had obtained the information in question from the Garda Commissioner at a time when he was Minister for Justice and Equality. Mr Wallace alleged that the information disclosed by Mr Shatter on Prime Time breached certain of his rights as protected under the Data Protection Acts, 1988 & 2003. In his decision on the complaint, the (then) Data Protection Commissioner upheld Mr Wallace's complaint, finding that Mr Shatter was a data controller in relation to the information in question and that, when he disclosed that information during the Prime Time programme, he had processed personal data relating to Mr Shatter in a manner which was incompatible with the purposes for which it had first been obtained. Mr Shatter appealed the Data Protection Commissioner's decision to the Circuit Court which dismissed the appeal by way of its judgment of 21 January 2015. An appeal against the Circuit Court decision was then brought by Mr Shatter. The case was heard in the High Court in July 2017 with a number of procedural and substantive issues raised. Mr Justice Meenan delivered his judgment on 9 November 2017 upholding Mr Shatter's appeal and finding on the substantive data protection issues that, amongst other things, Mr Shatter had not been a data controller for the purposes of the information relating to Mr Wallace which had been disclosed during the Prime Time programme and, further, that the information disclosed by Mr Shatter did not in fact comprise personal data relating to Mr Wallace.

(Note that this judgment may be subject to further appeal as the period for bringing an appeal from the High Court judgment has not yet expired as of the time of going to print).

Prosecutions Unit

Prosecutions were taken by the Data Protection Commissioner in 2017 under the Data Protection Acts 1988 and 2003 (the Acts), and under the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. 336 of 2011).

Six entities were prosecuted for offences under Regulation 13 of S.I. 336 of 2011 in respect of electronic marketing. The summonses for these six cases covered a total of 42 offences. Details of these prosecutions are set out in the Case Studies section.

With regard to prosecutions under the Acts, a private investigations company was prosecuted for offences under Section 22, and a director of that company was prosecuted for offences under Section 29. The summonses issued in respect of these prosecutions covered a total of 74 offences. Details of these prosecutions are set out in the section regarding Special Investigations Unit.

Binding Corporate Rules

Binding Corporate Rules (BCR) were introduced by the EU Article 29 Working Party in 2003, following discussions 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 a standard contractual clauses or approvals by several DPAs. The upcoming GDPR outlines in Article 47 how BCRs can continue to be used as an appropriate safeguard to legitimise transfers to Third Countries.

During 2017 the DPC acted as lead reviewer in relation to 14 BCR applications, a doubling of our 2016 numbers. Two of these were given final approval by us in 2017, Zendesk International Limited and Oracle EMEA Limited and the remainder will be finalised in 2018. We also acted as co-reviewer in three BCR applications assisting other lead reviewer DPAs with their approvals.

The referential documents for approval of BCR applications were updated in 2017 by the EU Article 29 Working Party with the input from the DPC to take into account GDPR requirements.

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 the DPC from May 2018.

DPC's Internal GDPR Readiness Programme

In early 2017, the DPC established a "Readiness Programme" in an aim to best prepare the organisation for its enhanced future functions as a regulator under the EU General Data Protection Regulation (GDPR), the Law Enforcement Directive, the Data Protection Act 2018 and the proposed ePrivacy Regulation. In addition to providing new protections for individuals, placing greater responsibilities on businesses to protect personal data, under this new legislation, the DPC will perform a range of new and enhanced regulatory functions to protect the rights of the public.

The Readiness Programme includes 28 workstreams that are led by senior members of the DPC and are supported by staff across the organisation. A steering group, comprising of the Commissioner and all Deputy Commissioners, ensure effective governance and oversight of each workstream through regular meetings and involvement in programme activities.

The programme workstreams continue to focus on driving internal readiness activity across a number of key areas including processes/procedures, IT/systems, people/organisation structure and corporate and compliance readiness.

Under this programme, during 2017 the organisation completed a 'Detailed Planning Phase' which involved significant work across the organisation to:

- review as-is processes/structures and ways of working to understand the scale of workload change that would be required under the new regulatory system;
- design and map critical future-state-processes across the organisation, including within the areas of assessment, complaint handling and investigation;
- explore and define the DPC's technical requirements in anticipation of implementing a new case management system to further support and embed enhanced management of complaints and investigations;
- analyse the potential workload impacts that the new regulatory system would have for the DPC and assess options to ensure a fit-for-purpose organisation; and

create a comprehensive plan of activities that would need to occur prior to the regulatory changes coming into effect.

Also during 2017, the programme transitioned into the 'Implementation Phase', with each workstream focussed on delivering the activities required for the DPC to effectively roll-out the new legislation. In particular, progress has been made to:

- further build GDPR awareness and readiness across the public and private sectors, for example, through a range of speaking events and public awareness campaigns;
- develop and implement new business processes to ensure that the DPC is ready to roll-out the new legislative requirements, including developing web-based forms to improve how the DPC engages with individuals and businesses, such as enabling organisations to submit breach notifications electronically;
- prepare the DPC to act as the 'Lead Supervisory Authority' in certain cross-border cases in alignment with the EU 'consistency mechanism', often referred to as the 'One-Stop-Shop';
- deliver a brand new user-friendly web-site providing information to members of the public and organisations regarding data protection and rebrand the DPC;
- develop and roll-out a new case management system to enhance how the DPC manages queries, complaints and investigations; and
- recruit new staff (with staff numbers almost triple what they were in 2014) and further enhance internal DPC capability through the training, development and up-skilling of staff.

In addition, during 2017 in preparation for GDPR implementation, the DPC continued to work with the Department of Justice and Equality to input into the general scheme and drafting of the Data Protection Bill 2018 (published in early 2018). Also, across the organisation, DPC staff engaged at EU level with the work being progressed by the Article 29 Working Group and its subgroups. The DPC Internal Readiness Programme will continue to be a priority during 2018 and will focus on ensuring DPC is well-prepared and fit for purpose leading up to 25th May 2018.

GDPR Awareness and Outreach

In 2017, the DPC took a leading role in raising awareness of the GDPR among industry and public-sector stakeholders, as well as the general public.

The DPC established a dedicated GDPR Awareness and Training unit, with responsibility for driving the DPC's GDPR awareness activities.

Central to the GDPR awareness drive was the launch of a GDPR micro-site, www.GDPRandYou.ie, serving as a central hub for organisations seeking assistance with GDPR preparations and a repository of guidance published by the DPC and the Article 29 Working Party.

The micro-site was launched one year out from GDPR, on 25th May 2017, along with a survey on levels of preparedness among small-to-medium enterprises. These results were used to inform the direction and content of subsequent DPC guidance in respect of GDPR. Guidance published in 2017 included a GDPR Readiness Guide, specifically targeted small-to-medium enterprises (SMEs), which comprised explanations and checklists designed to help the sector ensure its compliance under the GDPR.

Another key driver for our guidance in 2017 was generated from Q&A sessions and direct contact from our speaking engagements with stakeholders, which allowed us to gain insight into the data protection themes that our audiences were concerned with. Specifically, our engagement with the Small Firms Association (SFA) has helped ensure that Micro enterprises as well as SMEs are aware and prepared for their data protection responsibilities.

In addition to the micro-site and sector-specific guidance, the DPC also developed a digital video strategy — showcasing our mascot, Data Protection Dave — to help drive awareness of the GDPR and direct organisation to the information on the micro-site. Promoting the video on twitter resulted in viewer figures in excess of 1.4 million and high rates of click-through traffic to the www.GDPRandYOU.ie micro-site.

The clarity of the video's message and the success of its awareness remit were recognised as an industry-leading example of same, and was nominated for awards by the Irish Internet Association, Spider Awards and the inaugural International Conference of Data Protection and Privacy Commissioners (ICDPPC) Global Privacy and Data Protection Awards (education and advocacy category).

The video was the winner in its category at the IIA awards, and second in the ICDPPC awards.

The @DPCIreland Twitter account continues to maintain an active presence online, growing to 3,800 followers, and has proved to be an effective tool in disseminating the DPC's awareness activities to key stakeholders. Our Twitter account had almost 4 million impressions for the year.

Speaking Engagements

The DPC is committed to driving awareness of the GDPR. The office has maintained an active outreach schedule during 2017 and engaged with a broad base of Irish and international stakeholders. The Commissioner and her staff spoke and presented at events on almost 250 occasions in 2017, including conferences, seminars, and presentations to individual organisations from a broad range of sectors. Examples include:

- Data Summit (Dublin);
- The IBEC Regional Roadshow;
- 39th International Conference of Data Protection and Privacy Commissioners (Hong Kong);
- IBEC Annual Employment Law Conference;
- 9th Annual Sedona Conference (Maynooth);
- The Wheel;
- Sunday Business Post GDPR Compliance Summit;
- Cork Chamber of Commerce GDPR seminar for SMEs;
- House Meeting of the UCC Law Society;
- European Central Bank Data Protection Conference (Frankfurt);
- Law Society of Ireland Conferral Ceremony;
- 7th Annual European Data Protection Day Conference (Berlin);
- International Association of Privacy Professionals Congress (Brussels);
- International Association of Privacy Professionals Privacy Summit (Washington)
- Dublin Data Sec 2017;
- Cambridge Centre for Health Series research;
- Temple Street Foundation;
- Ploughing Championships; and
- International data protection conference hosted by Estonian EU Presidency (Tartu, Estonia).

Published Guidance

In addition to GDPR-specific guidance, in 2017 the DPC continued to publish guidance materials and blog posts on data protection related issues, including:

- E-receipts;
- Connected Toys;
- Ransomware; and
- Securing cloud-based environments.

In addition to the guidance generated in-house, the DPC worked closely with Retail Excellence and the Charities Regulator to produce targeted GDPR guidance for their respective sectors.

EU and International

EU cooperation

Article 29 Working Party

In 2017, DPC staff actively engaged in all of the Article 29 Working Party (WP29) Plenary and subgroups. The nine subgroups of WP29 cover a range of substantive topics, and includes one cooperation sub-group, which is tasked with overseeing any coordinated actions by DPAs, specifically those around the consequences of the Court of Justice of the European Union (CJEU) case which invalidated the Safe Harbour arrangement.

The other eight subgroups focus on these substantive issues:

- Enforcement
- The future of privacy;
- Key provisions;
- Technology;
- International transfers;
- Law enforcement (as well as borders and travel); and
- E-government and
- Financial matters.

The DPC as Lead Rapporteur for the Guidelines on Transparency under the GDPR and moderator at the Article 29 Working Party "Fablab"

Since the finalisation of the GDPR in the first half of 2016, much of the work of the Article 29 Working Party (WP29) has been focused on the preparation of guidance materials concerning the interpretation and application of key concepts and rules under the GDPR. One of the most significant changes to the rules on processing personal data under the GDPR is the introduction of the principle of transparency in Article 5.1. Reflective of the centrality of this principle, the WP29 has produced Guidelines on Transparency under the GDPR.

During the second half of 2017, the Commissioner's office acted as the WP29 "lead rapporteur" with responsibility for the drafting and preparation of these Guidelines, in conjunction with the other members of the WP29.

As part of our role as the lead rapporteur, senior staff members from the DPC moderated the WP29 "Fablab" on the topic of Transparency. The Fablab was a one-day consultation workshop event attended by EU industry and sectoral representatives, which was held in Brussels in October 2017 and focused on the separate topics of Transparency and International Transfers under the GDPR.

A preliminary version of the Guidelines on Transparency under the GDPR was published by the WP29 in December 2018 with a 6-week EU-wide consultation period following, for comments to be submitted to the WP29 on the Guidelines. The DPC will continue its work, as lead rapporteur, on these Guidelines during the first half of 2018, taking into account the outputs from the consultation, with a view towards finalising the Guidelines for formal adoption by the WP29 in April 2018.

The guidance published by the WP29 in 2017 included:

- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation;
- Guidelines on Personal data breach notification under Regulation;
- Guidelines on the application and setting of administrative fines;
- Guidelines on the Lead Supervisory Authority;
- Guidelines on Data Protection Officers ('DPOs');
- Guidelines on the right to "data portability";
- Guidelines on Data Protection Impact Assessment (DPIA);
- Opinion on key issues of the Law Enforcement Directive;
- Working documents on Binding Corporate Rules and Adequacy Referential;
- Opinion on personal data in the context of cooperative intelligent transport system; and
- Opinion on data processing at work.

European Guidelines for Codes of Conduct

Towards the end of 2017, the DPC became the lead rapporteur to draft European Guidelines for Codes of Conduct on behalf of the WP29. Codes of Conduct, as provided under Article 40 of the GDPR, will become a very important data protection tool, which can assist data controllers in demonstrating their compliance with the GDPR. Furthermore, adherence to a code of conduct will be a factor taken into consideration by a supervisory authority when evaluating the security of processing or when imposing an administrative fine. The intention of WP29 (which will become the European Data Protection Board under the GDPR) is to draft clear and practical guidelines, which will assist associations and representative bodies in drafting codes of conduct and provide supervisory authorities with a framework to evaluate codes consistently across Europe. It is envisaged that these guidelines will be approved and published by mid-2018.

EU Joint Supervisory Bodies

During 2017, we continued to participate in the work programmes of the Europol Co-Operation Board, Joint Supervisory Body of Eurojust and the European Data Protection Supervisory Groups for Eurodac, Customs and the Internal Market Information (IMI) database. In line with our supervisory powers, we conducted a desk audit of Eurodac in 2017.

International Co-operation

Memoranda of Understanding

The global nature of many cases investigated by the DPC means international cooperation is a necessity for effectiveness. During 2017, information sharing with the Federal Trade Commission in the US and the Privacy Commissioner of Canada were of particular utility in progressing issues.

Spring Conference of European Data Protection Authorities

The Spring conference for 2017 was hosted by the Cypriot Data Protection Authority. They organised an impressive and valuable conference bringing together European data protection authorities and policy makers. The DPC was pleased to have been invited to be a panellist on the topic of Data Protection and Cloud Computing at the conference and benefitted overall from renewed contact with our fellow data protection authorities at the event.

British Irish and Islands' Data Protection Authorities Conference

Gibraltar was the venue for the 2017 conference of the British Irish and Islands' Data Protection Authorities Conference. Comprising the data protection authorities of Ireland, the UK, Cyprus, Malta, Isle of Man, Gibraltar and Bermuda, the focus of the 2017 event was the GDPR which provided a timely and valuable opportunity for participants to exchange useful information on our respective GDPR readiness programmes.

International Conference of Data Protection and Privacy Commissioners

"East meets West" was the theme of this year's conference in Hong Kong. The plenary and side events were of very high quality in terms of learning and engagement and the DPC was pleased to be invited to participate and contribute on panels at both. The conference was very well attended by EU and data protection authorities worldwide – almost all were in attendance — and it again provided a useful forum to better our understanding of each other's authority, processes and underpinning legislation. The GDPR demands increased cooperation within the EU between EU authorities and the extra territorial reach of the Regulation will also demand enhanced cooperation with authorities worldwide. These types of events assist in bringing together the national authorities and uniting them around common data protection themes and challenges.

International delegations

During 2017, the DPC had the privilege of hosting visits from the Estonian, UK and Japanese Data Protection Authorities and the Turkish Social Security Agency. These dialogues included discussions on the implementation of the GDPR, global data protection issues and cooperation between data protection authorities.

Registration

Under the Data Protection Acts 1988 and 2003, certain categories of data controllers and processors are legally bound to register with the DPC on an annual basis.

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

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

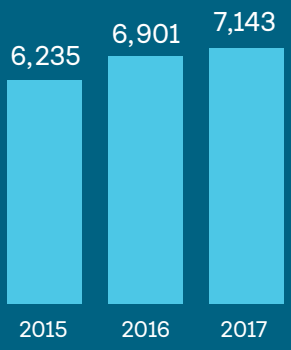
Registration should not be interpreted as automatically deeming an organisation to be fully data protection compliant by virtue of having their registration entry up to date. Data controllers, regardless of whether they are required to register, are bound by the data protection responsibilities set out in the Data Protection Acts.

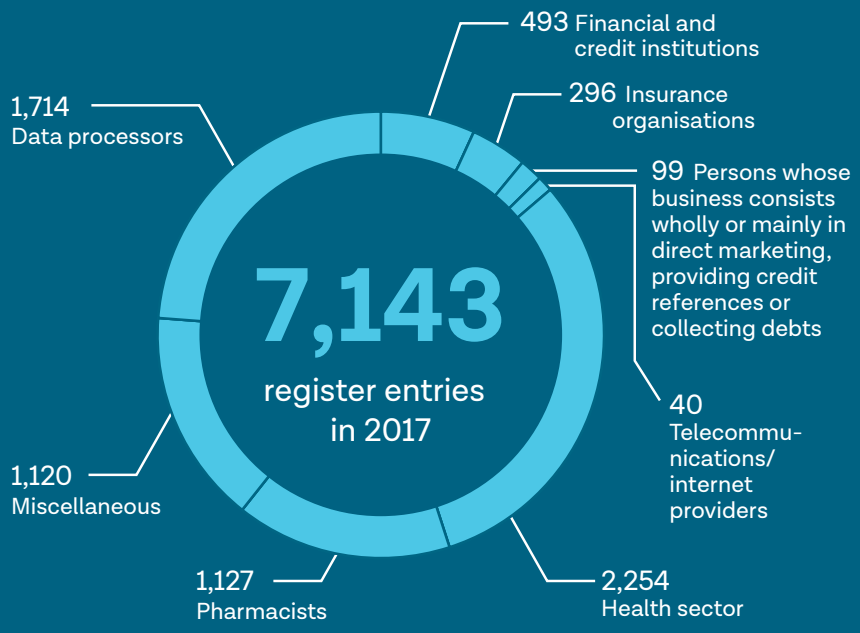
The total number of register entries in 2017 was 7143, as follows:

Category	Number
Financial and credit institutions	493
Insurance organisations	296
Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts	99
Telecommunications/internet providers	40
Health sector	2254
Pharmacists	1127
Miscellaneous	1120
Data processors	1714

Registration will no longer be a legal requirement from 25 May 2018 when the General Data Protection Regultion comes into effect.

Registration Entries 2015–2017





Corporate Affairs

Overview

The Corporate Affairs division of the DPC is responsible for the developing and implementing measures to ensure organisational compliance with legislative and corporate governance requirements. In addition, the division is responsible for supporting achievement of the organisation's strategic and operational objectives through ensuring that financial, administrative, HR and ICT services are in place.

Finance

Government funding of the DPC has increased significantly in recent years from €1.7 million in 2013 to an allocation of €7.52 million in 2017 (comprising €5.16m pay and €2.36m non-pay).

The DPC acknowledges the significant increase in funding in recent years and welcomes the Government's continuing commitment to ensuring that the DPC is appropriately resourced to fulfil its mandate as the independent supervisory body in Ireland charged with upholding the EU fundamental right to data protection.

The budget for the DPC is channelled through the vote of the Department of Justice and Equality 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 expenditure and approval limits that apply across the Department of Justice and Equality and also observes the requirements set out in Public Financial Procedures and the Public Spending Code.

The DPC avails of shared services for its payment and accounting processes. Invoice payments are processed through the central accounting system in the Department of Justice and Equality's Financial Shared Services Centre (FSS). The Payroll Shared Service Centre (PSSC) processes payroll and expense payments, which is under the remit of the Department of Public Expenditure and Reform (DPER).

During 2017, the DPC also had an allocation for receipts to be collected in respect of organisations required to register as data controllers and/or data processors under the Data Protection Acts 1988-2003. Such receipts were transferred directly to the Exchequer throughout the accounting year. Under the GDPR, from May 25th 2018, there will no longer be a requirement for registration by data controllers and processors.

2017 Annual Financial Statement

The 2017 Account of Income and Expenditure is currently being prepared and will be submitted to the Comptroller & Auditor General for audit. Once the audit is concluded and the annual financial statement has been approved by the C&AG, the 2017 Financial Accounts will be appended to this report.

Staff Resources

The Data Protection Commissioner is appointed by Government in accordance with the Data Protection Acts, and is independent in the exercise of her functions.

As outlined above, the additional annual budget resources allocated to the DPC in recent years have facilitated the significant expansion of the DPC's staffing with an emphasis on strengthening the organisation's skills base in the areas of legal, technology, audit and investigations.

Throughout 2017, staff recruitment was a high priority for the DPC, and the organisation, working effectively with the Public Appointments Service, recruited over 30 new staff through open and through a number of specialised recruitment campaigns. Consequently, the DPC staff allocation has almost tripled in size since 2014 with staffing levels at the end of 2017 having increased to approximately 85 staff across our offices in Dublin and Portarlington.

The DPC is staffed by civil servants who work in accordance with the Civil Service Code of Standards and Behaviours, as well as corporate policies, procedures, and circulars. Staff training and continuous development is a key priority for the DPC. Staff received internally and externally provided training throughout 2017. We held four 'Communications Days', on a quarterly basis, which enabled upskilling and capacity building of staff, including preparing for the GDPR.

Recruitment will continue to be a priority into 2018 and the organisation will continue to grow in the period up to and following 25 May 2018 to ensure that it has the capacity to effectively carry out the broad range of tasks and functions required under the new EU General Data Protection Regulation and national legislation.

Corporate Governance

Code of Practice for the Governance of State Bodies

As an independent body, the DPC continues to develop its corporate governance structures and procedures to ensure it applies high standards of corporate governance aligned with the requirements set out for all public sector bodies 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 put in place a Corporate Governance Assurance Agreement with the Department of Justice & Equality. The Agreement sets out the broad corporate governance framework within which the DPC operates and defines key roles and responsibilities that underpin the relationship between the 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 the GDPR, it is not subject to a Performance Delivery Agreement with the Department of Justice & Equality.

In accordance with the Code of Practice, the DPC's Statement of Internal Controls is included at Appendix V.

Statutory Governance Requirements

The Data Protection Commissioner is responsible for the preparation of the Annual Report and the Financial Statements in accordance with the provisions of the Data Protection Acts 1988 and 2003 (Section 14 and Schedule 2 (9) respectively).

All expenditure of the DPC is accounted for to the Exchequer, and the Comptroller and Auditor General audit the organisation's accounts annually. Our daily interaction with citizens, businesses and other key stakeholders provides additional oversight of the work we undertake. In addition, statutory decisions of the Commissioner can be appealed to the Courts.

The 2017 Annual Financial Statements will be appended to this Annual Report once the C&AG audit had been completed.

Strategic Planning

The DPC carries out its functions in accordance with the provisions of the Data Protection Acts 1988 and 2003, and the key strategic goals set out in our Statement of Strategy 2017-2018. The delivery of our remit in 2017 was underpinned by divisional business plans and the individual goals of staff members. Our Statement of Strategy will be reviewed in late 2018 following the implementation of the GPDR, and a new strategy for the period 2019-2021 will be prepared.

Risk Management

The DPC operates a formal Risk Management policy and maintains a Risk Register in accordance with the Department of Finance guidelines, which is maintained on an ongoing basis. The maintenance of the register is designed to ensure that risks are identified and assessed and necessary mitigating actions, when necessary, are put in place. The Risk Register is compiled on behalf of the Senior Management Committee (SMC) and reviewed by the members of the SMC on at least a quarterly basis.

Reflecting the key priorities for the organisation, the main risks managed by the office are as follows:

- building organisational capacity including enhancing the expertise of the DPC's staff and the recruitment of new staff with specialist investigatory, legal and information technology skillsets, in light of the new and enhanced functions of the organisation under the GDPR and national legislation;
- ensuring effective integration and consolidation of new structures, functions and business processes across the organisation as the DPC prepares to take on new and enhanced supervisory functions and responsibilities set out by the GDPR;
- ensuring that appropriate internal controls and new business processes are in place to directly manage functions such as financial, HR, Payroll, ICT, and internal audit as the DPC transitions to a 'Scheduled Office' with its own Vote and Accounting Officer in the course of 2018/2019; and
- ensuring that the DPC has effective and efficient 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.

Audit

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). 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 2017 and the audit report was considered before the SMC and the DJE Audit Committee. The audit did not identify any significant issues.

The DPC received one request in 2017 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. The review upheld the original decision to refuse access to the information requested. The matter has since been appealed to the Commissioner for Environmental Information.

Senior managers from the DPC attended an Audit Committee meeting in 2017 to discuss audit related matters. The DPC provided the Committee with an update on ongoing strategic and operational reforms across the organisation. These reforms will help mitigate risks and ensure that the DPC can deliver on its mandate.

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. An overview of these requests is provided as follows:

The Information Commissioner made a decision in February 2017 in relation to an application for review, made by Right To Know CLG (the applicant), arising out of the DPC's refusal of the applicant's request for access to records relating to a number of entries in the Register of Lobbying. The Information Commissioner upheld the DPC's decision to refuse the request, finding, amongst other things, that the records in question did not concern the general administration of the office of the DPC and, as such, the DPC was justified in refusing the request under the Freedom of Information Act 2014. The decision of the Information Commissioner (No. 160447) is available on the Information Commissioner's website.

2017 Freedom of Information Requests

Requests by Type	Category Total	Outcome
Relating to administrative issues	2	Granted
Relating to personal data (outside of scope)	11	Refused / Not accepted
Relating to matters outside of the scope of the Acts	30	Refused / Not accepted / Handled outside FOI
Live Cases	1	Awaiting decision as of Dec 31st
Overall Total	**44**	

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 an Irish language service as per our Customer Charter, and Irish language information via our website.

Appendix I

List of Organisations Audited or Inspected in 2017

The Commissioner would like to thank all of those organisations audited and inspected throughout the year for their cooperation. The inspection teams found that 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.

- AIG (Telematics)
- Survey Monkey
- GoHop
- LinkedIn Ireland Ltd.
- Avoca
- Tesco
- St Patricks Accommodation Centre
- Elverys
- Irish Foster Care Association
- Mosney Accommodation Centre
- Coláiste Chill Mhantáin
- Isaacs Hostel
- Egali Hostel
- Blooms Hotel
- Three
- Family Carers Ireland
- NCT Call Centre
- Debenhams
- New Look
- D.I.D. Electrical
- Lemap Ltd. t/a Diesel
- Dublin Airport Carlton Hotel
- Eurodac (desk based audit)
- Portiuncula University Hospital
- Oasis
- Athlone Accommodation Centre
- Gresham Hotel
- Jurys Inn Christchurch
- Irish Life Health
- Early Childhood Ireland
- Threshold
- Malahide Public Library
- Sonas

- Barnardos
- Dept Agriculture — KT Scheme
- Dublin Coach
- Seetec (JobPath)
- Turas Nua (JobPath)
- Virgin Media
- Matthews.ie
- Event Strategies Ltd.
- South Infirmary Victoria University Hospital
- National Medical Card Unit
- BT Ireland
- Irish Prison Service (Prisoner Information Management System)
- Hooke & McDonald (Lettings Agent)
- Savills (Lettings Agent)
- Central Bank (Central Credit Register)
- National Asset Management Agency (NAMA)
- Transgender Equality Network Ireland (TENI)
- Dublin City Council
- Hibernia College Dublin
- Health Service Executive (Byrne Wallace Solicitors on its behalf)
- Capita Asset Services, Dublin 2
- Dr. O'Droma, Orthocosmetics, Howth, Co. Dublin
- SIU Inspections (Special Investigations Unit)
- Midlands Regional Hospital, Mullingar
- Synergy Credit Union
- Aut Even Hospital, Kilkenny
- Royal Victoria Eye and Ear Hospital
- Mater Misericordiae University Hospital
- Dublin Motor Taxation Office
- Beaumont Hospital
- Our Lady's Children's Hospital, Crumlin
- Adelaide & Meath Hospital, incorporating the National Children's Hospital (Tallaght Hospital)
- St. Luke's Hospital, Kilkenny
- An Garda Síochána, Garda Headquarters, Phoenix Park
- Cork University Hospital
- Our Lady's Hospital, Navan
- Naughton Consultancy Services, Rathfarnham, Dublin 16
- Jim McNulty Security and Surveillance Services
- University Hospital Kerry, Tralee
- Wexford General Hospital
- University Hospital Galway
- Department of Social Protection, Mallow
- Tusla Child and Family Agency, Limerick
- Tusla Child and Family Agency, Tralee
- University Hospital Limerick
- Private Investigation, Celbridge
- Tusla Child and Family Agency, Kilkenny
- Sligo University Hospital, Sligo
- Tusla Child and Family Agency, Our Lady of Lourdes Hospital, Drogheda
- Tusla Child and Family Agency, Gaolta Centre, Drogheda
- Tusla Child and Family Agency, Navan, Co. Meath
- Letterkenny University Hospital, Co. Donegal
- Tusla Child and Family Agency, Churchtown, Dublin 12
- Blackrock Clinic, Blackrock, Co. Dublin
- Tusla Child and Family Agency, Portlaoise
- Bons Secours Hospital, Cork
- Tusla Child and Family Agency, Heuston South Quarter, Dublin 8
- National Maternity Hospital, Holles Street, Dublin 2
- St Vincent's University Hospital, Elm Park, Dublin 4

Appendix II

Case Studies

CASE STUDY 3: Loss of sensitive personal data contained in an evidence file kept by An Garda Síochána

We received a complaint from a couple against An Garda Síochána (AGS), concerning the loss of an evidence file that held, among other things, the couple's sensitive personal data relating to details of medical treatment. We established that the couple had previously made a criminal complaint to AGS and had subsequently made an access request. However, in response to the access request, they were informed that the evidence file in relation to their complaint, which contained their original statements, a DVD and postal documents containing their sensitive personal data, had been misplaced while in the possession of AGS. The complainants requested that we conduct a formal investigation into the matter.

AGS informed us that upon identifying that the evidence file in question was missing, a comprehensive search had taken place of all files retained at local level in the District Office, and other relevant sections of AGS, in order to try to locate the file. Ultimately, however, the file had not been located.

During the course of our investigation, we studied the chain of custody supplied to us by AGS and established that the last known whereabouts of the file was in the investigating officer's possession. That officer had been instructed by a superior to update the couple about the criminal complaint and to then return the file to the District Office for filing. However, the officer had failed to return the file to the District Office for filing. AGS informed us that the failure by the officer to return the file to the relevant location in the District Office was in contravention of its policy and procedures at the time and that consequently both an AGS internal investigation and a Garda Síochána Ombudsman Commission investigation had been conducted. Following the latter investigation, the officer in question had been disciplined and sanctioned for the contravention.

One of the central requirements of data protection law is that data controllers have an obligation to have appropriate security measures in place to ensure that personal data in their possession is kept safe and secure. This requires the controller to consider both technical and organisational measures and importantly, to take all reasonable steps to ensure that its employees, amongst others, are aware of and comply with the security measures. In her decision, the Commissioner found that AGS, as data controller, had infringed Section 2(1)(d) of the Data Protection Acts 1988 and 2003, as it failed to take appropriate security measures to ensure the safe storage of the complainants' sensitive personal data which was contained on the evidence file in question.

This case demonstrates that the obligation on a data controller to maintain appropriate security measures goes beyond simply putting in place procedures regarding the storage and handling of personal data. Such procedures are only effective as a security control if they are consistently adhered to, so data controllers must monitor staff compliance with these measures and take meaningful steps (for example training, auditing and potentially disciplinary measures where non-compliance is identified) to ensure that staff systematically observe such procedures.

CASE STUDY 4: Use of CCTV footage in a disciplinary process.

We received a complaint from an individual regarding the use of CCTV footage by their employer in a disciplinary process against them. The complainant informed us that while employed as a security officer, their employer had used their personal data, in the form of CCTV footage, to discipline and ultimately dismiss them. The complainant stated that they had not been given prior notification that CCTV footage could be used in disciplinary proceedings.

In the course of our investigation, the employer informed us that the complainant had worked as a night officer assigned to client premises, and had been required to monitor the CCTV system for the premises from a control room. The employer's position was that, upon being assigned to the client premises in question, the complainant had been asked to read a set of "Standing Operating Procedures" which indicated that CCTV footage could be used in an investigative process concerning an employee. The employee had also been asked to sign a certificate of understanding to confirm that he had read and understood his responsibilities. The employer maintained that the CCTV system in place at the client premises was not used for supervision of staff as there was a supervisor at the premises during office hours between Monday and Friday.

The employer informed our investigators that it was the complainant's responsibility, as the sole night security officer on duty at the client premises, to monitor the CCTV system for the premises from the control room. The requirement to have a night security officer on duty in that control room for that purpose was a term of the

employer's contract with its client. The employer was also contractually obligated under its contract with its client to carry out routine audits of employee access cards (which were swiped by the holder to gain access to various locations in the client premises). The employer told us that during such an audit, it had discovered irregularities in data derived from the complainant's access card which could not be the result of a technical glitch as those irregularities were not replicated in the access card data of the complainant's fellow night officers. These irregularities suggested that the complainant had been absent from their assigned post in the control room for prolonged periods of time on a number of separate occasions. On the basis of the access card data irregularities and upon noting the apparent absence of the employee from the control room during prolonged periods, the employer had commenced an investigation into the employee's conduct. During the course of this investigation, the complainant disputed the accuracy of the access card data, and had sought that the employer provide further evidence of his alleged prolonged absences from the control room. The employer had therefore obtained CCTV stills at times when the access card data suggested the complainant was away from their post in order to verify the location of the complainant. The employer maintained that because the CCTV system was independent of the access card data system, it was the only independent way to verify the access card data. The employer also provided us with minutes of a disciplinary meeting with the complainant where they had admitted to being away from the control room for long periods. The employer also informed us that the complainant had later admitted in an email, also provided to us, that the reason for these absences was that the complainant had gone into another room so that they could lie down on a hard surface in order to get relief from back pain arising from a back injury.

We queried with the employer what the legal basis was for processing the complainant's personal data from the CCTV footage. The employer's position was that as a result of its contractual obligations to its client (whose premises were being monitored), if an adverse incident occurred during a period of absence of the assigned security officer (the employee) from the control room, that would potentially expose the employer to a breach of contract action by its client which could lead to significant financial and reputational consequences for the employer. On this basis the employer contended that it had a legitimate interest in processing CCTV footage of the employee for the purpose of the disciplinary process.

Under Section 2A(1)(d) a data controller may process an individual's personal data, notwithstanding that the controller does not have the consent of the data subject, where the processing is necessary for the purposes of the legitimate interests pursued by the data controller. However, in order to rely on legitimate interests as a legal basis for processing, certain criteria have to be met as follows:

- there must be a legitimate interest justifying the processing;
- the processing of personal data must be necessary for the realisation of the legitimate interest; and
- the legitimate interest must prevail over the rights and interests of the data subject.

Having considered the three step test above, the Commissioner was satisfied that the employer had a legitimate interest in investigating and verifying whether there was misconduct on the part of the employee (or whether there was a fault in the access card security system). Furthermore, the Commissioner considered that the use of the CCTV footage was necessary and proportionate to the objective pursued in light of the seriousness of the allegation because it was the only independent method of verifying the accuracy of the access card data. The Commissioner noted that the CCTV footage was used in a limited manner to verify other information and that the principle of data minimisation had been respected. Finally, given the potential risk of damage to the employer's reputation and the need to ensure the security of its client's premises, the Commissioner was satisfied that the use of CCTV footage for the purpose of investigating potential employee misconduct, which raised potential security issues at a client premises, in these circumstances took precedence over the complainant's rights and freedoms as a data subject. On the issue of whether the controller had provided the complainant with notice of the fact that their personal data might be processed through the use of CCTV footage, the Commissioner was satisfied that there had been adequate notice of this by way of the SOP document which had been acknowledged by the complainant signing the certificate of understanding.

This Commissioner therefore formed the view that the employer had a legal basis for processing the complainant's personal data contained in the CCTV footage under Section 2A(1)(d) of the Data Protection Acts 1988 and 2003.

This case demonstrates that the legal basis of legitimate interests will only be available to justify the processing of personal data where, in balancing the respective legitimate interests of the controller against the rights and freedoms of the data subject, the particular circumstances of the case are clearly weighted in favour of prioritising the legitimate interests of the controller. It is an essential that in order to justify reliance on this legal basis that the processing in question is proportionate and is necessary to the pursuit of the legitimate interests of the controller.

CASE STUDY 5: Disclosure of sensitive personal data by a hospital to a third party

We received a complaint concerning the alleged unauthorised disclosure of a patient's sensitive personal data by a hospital to a third party. The complainant had attended the hospital for medical procedures and informed us that the medical reports for these procedures were received to their home address in an envelope that had no postage stamp. The envelope had a hand-written address on it which included the name of a General Practitioner (GP) and also included the home address of the complainant's neighbour. A hand-written amendment had been made to the address, stating that it was the wrong address. The complainant informed us that they had made enquiries with their neighbour in relation to the correspondence and the neighbour had stated that they had received the correspondence a number of days prior but that it had not been delivered by a postman. The neighbour further advised the complainant that they opened the envelope and viewed the contents in an effort to locate the correct recipient/address.

Following the initial complaint, the complainant provided us with correspondence which they subsequently received from the hospital apologising that correspondence containing the complainant's medical results had been inadvertently sent to the wrong address. The hospital indicated that this appeared to have been due to a clerical error confusing part of the GP's address and part of the complainant's address. We commenced an investigation to establish how the error had happened, what procedures the hospital had in place at the time and what the hospital since had done to avoid repetition of this incident.

The hospital informed us that their normal procedure is to issue medical reports in batches to the relevant GP so that multiple sets of medical reports for different patients are placed in a windowed envelope, which shows the relevant GP's address in the window. In this case however, the medical report was put in a non-windowed envelope and the address was hand-written on the front. In doing so, the staff member who had addressed the envelope manually, erroneously intermixed the GP's name, part of the GP's address and part of the complainant's address on the envelope. The hospital also informed us that the envelopes containing results to be dispatched to GPs are franked by the hospital post room. However, in this case because the envelope containing the complainant's medical information was not franked, the hospital concluded that it was unlikely that it had been sent out directly from their post room and indicated that it could have been sent on via the relevant GP, although they acknowledged that they could not be certain about this this. We were unable to establish during the course of the investigation the precise manner in which the envelope containing the complainant's medical reports came to be delivered to the complainant's neighbour's house. The hospital informed us that administrative staff had since been briefed on the correct procedure for issuing medical reports and that non-window envelopes would no longer be used for this purpose.

The complainant rejected the apology from the hospital made by way of an offer of amicable resolution and instead requested a formal decision from the Commissioner. In her decision, the Commissioner found that the hospital had contravened Section 2(1)(b) (requirement to keep personal data accurate, complete and up to date), Section 2(1)(d) (requirement to take appropriate security measures) and Section 2B(1) (requirement for a legal basis for processing sensitive personal data) of the Data Protection Acts 1988 and 2003 when it processed the complainant's sensitive personal data by way of disclosing their personal data inadvertently to a third party.

This case illustrates how a seemingly innocuous deviation by a single staff member from a standard procedure for issuing correspondence can have significant consequences for the data subject concerned. In this case, highly personal medical information was accessed by a third party in circumstances which were entirely avoidable. If the hospital had had in place appropriate quality control and oversight mechanisms to ensure that all staff members rigidly adhere to its standard procedures it unlikely that this unauthorised disclosure of sensitive personal data would have occurred.

CASE STUDY 6: Publication of personal information — journalistic exemption

We received a complaint concerning an article published in the Sunday World (in both newspaper and online news forms) which named the complainant and published their photograph. The focus of the article was official complaints made by Irish prisoners under the Prisons Act 2007 concerning their treatment in prison (known as "Category A" complaints) and it included details of the number of "Category A" complaints which had been made by the complainant. It was alleged by the complainant that the Sunday World had gained unauthorised access to their personal data from the Irish Prison Service.

The complainant provided us with a letter which they had written to the editor of the Sunday World asserting that the information contained in the article was inaccurate and violated their right to privacy and requesting that the link to the online article be removed. We were also provided with a previous decision of the Press Ombudsman which dealt with various alleged breaches of the Code of Practice of the Press Council of Ireland (the Code) by the Sunday World, including allegations of breaches arising from the article in question. The Press Ombudsman had decided that there had been a breach of Principle 5 of the Code concerning privacy and that the article could have been written without publishing the complainant's name or photograph. The position taken by the Press Ombudsman was that as "Category A" complaints are not part of the public record, the complainant's reasonable expectation of privacy had been breached by the publication of their name and photograph.

In the course of our investigation we queried with the Sunday World why it had not removed the online version of the article from its website in light of the Press Ombudsman's decision and in light of the complainant's written request to do so. We also queried how the Sunday World had obtained the complainant's personal data. In its response, the Sunday World stated its position that the publication was in the public interest as it related to the regimes of care and management of inmates as well as staff of prisons. It also contended that the article had highlighted how the [complaint] system was being deliberately over-used and abused. The Sunday World informed us that the online version of the article had been removed upon receiving the formal request from the complainant. However, the Sunday World relied on the journalistic exemption provision under Section 22A of the Data Protection Acts 1988 & 2003 (the Acts) in relation to the obtaining of the information in relation to the "Category A" complaints and the complainant's personal data.

The Commissioner issued a formal decision in relation to the complaint and specifically in relation to the application of Section 22A exemption. The rationale behind the exemption in Section 22A is to reconcile the protection of privacy and freedom of expression. Following the entry into the force of the Lisbon Treaty, data protection acquired the status of a fundamental right. The right to freedom of expression is also a fundamental right. Both rights are also recognised in the European Convention on Human Rights, and also referred to in the EU's Data Protection Directive 95/46/EC which is given effect in Irish law through the Acts.

Section 22A of the Acts specifies that personal data that is processed only for journalistic purposes shall be exempt from compliance with certain provisions of that legislation (including the requirement to have a legal basis for processing the personal data) provided that three cumulative criteria are met. Under Section 22A(1)(b), one of these three criteria is that the data controller, in this instance the Sunday World, must reasonably believe that, having regard in particular to the special importance of the public interest in freedom of expression, such processing (in this case by way of publication in the newspaper) would be in the public interest. The Sunday World claimed that the purpose of the article in question was essentially to highlight what it perceived to be an abuse of process within the Irish Prison Service. In her decision, the Commissioner found that it was not reasonable for the data controller to believe that the processing of the complainant's personal data by publishing their name and photograph would be in the public interest in achieving the stated objective of the Sunday World. It was the view of the Commissioner that the special importance in freedom of expression could have been satisfied had the journalist in question used other means to reach the desired objective for example by using statistics in relation to the number of 'Category A' complainant prisoners and the public interest had been neither enhanced nor diminished by identifying the complainant by means of their name and photograph. As one criterion out of the three cumulative criteria for the application of the journalistic exemption under Section 22A of the Acts had not been satisfied, the Commission found that it was not necessary to consider the remaining two criteria.

As the data controller was unable to rely on Section 22A of the Acts as an exemption from the requirement to have a legal basis for processing by publishing the complainant's personal data, the Commission in her decision then went on to consider whether there was in fact such basis for the processing. While the Commission considered that the Sunday World had a legitimate interest in obtaining and processing statistical information in relation to 'Category A' complaints for the purpose of research for the article in question, she considered that the Sunday World had contravened Section 2(1)(c)(iii) by further processing the complainant's personal data, through publishing it. This contravention arose as the processing of the data by publication was excessive and unnecessary for the purpose of the point being made by the Sunday World in the article i.e. that the system was being abused.

This case illustrates that the journalistic exemption under Section 22A of the Acts is not a blanket exemption that can be routinely relied on by publishers or journalists seeking to justify publishing unnecessary personal data. The mere existence of a published article is not sufficient to come within the scope of this exemption and instead a data controller must be able to demonstrate that they satisfy all three cumulative criteria in this section, as follows:

(i) the processing is undertaken solely with a view to the publication of journalistic, literary or artistic material;

(ii) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, such publication would be in the public interest; and

(iii) the data controller reasonably believes that, in all the circumstances, that having to comply with the relevant requirement of the Acts would be incompatible with journalistic, artistic or literary purposes.

CASE STUDY 7: Compliance with a Subject Access Request & Disclosure of personal data/ capture of images using CCTV

We received a complaint from an individual employed as a service engineer by a company, which was contracted to provide certain services to a company which was the operator of a toll plaza (the Toll Company). The complainant alleged, amongst other things, that the Toll Company had disclosed the complainant's personal data (consisting of an audio recording and CCTV footage of a conversation between the complainant and an individual operating a tollbooth at the toll plaza) to the complainant's employer without the complainant's knowledge or consent.

During our investigation we established that an incident had occurred involving the complainant resulting in a request being made by the Toll Company to the complainant's employers that the complainant was not to attend the toll plaza premises again in his capacity as a service engineer. We established that the incident in question involved a dispute at a toll both between the complainant and an individual operating the toll both, over the price of the toll which the complainant was charged. The Toll Company alleged that during the incident in question (which had been captured on CCTV and by audio recording) the complainant had threatened to "bring down" the toll plaza system. The complainant's employer had confirmed that it would comply with the Toll Company request that the complainant not attend the toll plaza premises again and the Toll Company confirmed to us that at that point it had considered the matter to be concluded. However, approximately two months after the incident had occurred, the complainant's employers had requested the CCTV footage and audio recording of the alleged incident which the Toll Company then provided to the employer. It was contended by the Toll Company that it was in its legitimate interests to process the complainant's personal data as a threat to it had been made by the complainant and that one its employees had reported the threat to the Gardaí, who had been called to the toll plaza by the complainant at the time of the incident. The Toll Company also claimed that Sections 8(b) and Section 8(d) of the Data Protection Acts 1988 and 2003 (the Acts) allowed for this processing of the complainant's personal data as the processing was necessary to prevent damage to the Toll Company's property. The Company stated that the personal data of the complainant (the CCTV footage

and audio recording) had been sent to the complainant's employer two months after the incident as it had not been requested by the employer prior to that.

As part of our investigation, we noted that signs at the tollbooth notified the public that there was CCTV in operation. We also examined the Toll Company's data protection policy which was available on its website and which stated that all vehicles using the toll plaza in question are photographed/video recorded and that images are retained for enforcement purposes and to address and resolve any disputes that may arise in relation to a vehicle or account.

In her decision, the Commissioner considered the Toll Company's purported reliance on pursuit of its legitimate interests as the legal basis under Section 2A(1)(d) of the Acts for the processing. Taking account of the two-month period which had elapsed between the incident in question and the request for the CCTV footage and audio recording being made by the employer, and also having regard to the confirmation of the Toll Company that (prior to receiving the employer's request for the CCTV footage and audio recording) it had considered the incident to be concluded, the Commissioner decided that this legal basis could not be relied upon for the processing of the personal data. Consequently, a contravention of Section 2A(1) occurred as there had been no other legal basis (e.g. the consent of the complainant) to the processing of his personal data by disclosing it to his employer. The Commissioner also found that there was no adequate notice of the processing of the personal data had not been to the complainant, as it was not apparent from the data protection privacy policy or indeed the public signs at the tollbooth what the extent of the processing was, that audio recording was in operation nor was it stated who the data controller was. Consequently the Toll Company had contravened Section 2D(1) arising from this lack of transparency. Finally, the Commissioner also found that Section 2(1)(c)(ii) of the Acts had been contravened because further processing of the complainant's personal data had occurred for a purpose (sharing it with the complainant's employer) which was incompatible with the original purpose for its collection (enforcement purposes and resolving

This case is indicative of a common trend amongst data controllers to seek to rely on legitimate interests as the legal basis for processing personal data as something of a catch-all to cover a situation where personal data has been processed reactively and without proper consideration having been given in advance as to whether it is legitimate to carry out the processing. However, as this case illustrates a data controller must be able to provide evidence to support their assertion as to the legitimate interest relied on. Here, the passage of time since the incident and the fact that the data controller of its own admission considered that the matter had been concluded contradicted the purported reliance on this legal basis. This case also underscores the principle of the foreseeability of processing of personal data as an important element of the overarching principle of fair processing in data protection. At its core this means that a data subject should not be taken by surprise at the nature, extent or manner of the processing of their personal data.

CASE STUDY 8: Failure to respond fully to an access request

We received a complaint that an educational organisation had not fully complied with an access request submitted to it by the complainant who was an employee of that organisation. The complainant informed us that in the access request they had specifically sought CCTV footage from the educational organisation's premises for 4 hour period during which the complainant had allegedly been assaulted by another employee. The complainant informed us that although there were 8 cameras on the premises, in response to their access request they only received an 11 second clip from the CCTV footage for the premises which ended just as the alleged assault came into view. The complainant told us that they had queried the limited amount of CCTV footage and reminded the educational organisation that the access request had been in respect of all footage within that 4 hour period. However, the educational organisation's response had been that this query would be treated as a new access request. The complainant considered that the CCTV footage had been intentionally withheld and that this approach had been adopted as a delaying tactic so that the CCTV footage would ultimately not have to be released on the grounds that it had been lost or was no longer retained.

In the course of our investigation, we established that the complainant had made a subject access request to the educational organisation which had accepted it as a valid request. The educational organisation's position was that it understood the complainant's request to relate to footage of the incident in question only. However, the educational organisation acknowledged

that the complainant would have been captured by other CCTV cameras for which the CCTV footage had not been provided. On this basis, we established that, as of the date of the complainant's access request, additional personal data existed in the form of further CCTV footage which had not been provided to the data subject. The educational organisation informed us that as the CCTV was only retained for 28 days, by the time that the complainant had come back to query the limited amount of CCTV footage received in response to the access request, the additional CCTV footage had been subsequently overwritten without being retained for release to the complainant.

In her decision the Commissioner noted that it was clear that in the complainant's access request the complainant was specifically seeking access to CCTV footage over a four-hour period and that having received the initial request, the educational organisation should have preserved the footage for that date and sought to clarify with the complainant what CCTV footage exactly they were seeking rather than unilaterally determining that issue itself. The educational organisation therefore contravened Section 4 of the Data Protection Acts 1988 and 2003 in failing to provide the complainant with all of their personal data within the statutory 40-day period.

This case clearly illustrates the position of the DPC which is that upon receipt of an access request relating to CCTV footage from a specific day, a data controller is obliged to preserve any such footage from that day pending resolution of the access request. This obligation applies irrespective of whether any such footage may be ordinarily subject to deletion (whether automated or not) after certain timeframes under the provisions of the data controller's retention policy. Where a data controller considers that further clarification should be sought from the data subject as to the scope of the personal data requested, that requirement for clarification should not be interpreted as if the access request had not yet been made, as to do so could undermine the data subject's right to access their personal data or enable a data controller to circumvent its obligations in respect of the access request.

CASE STUDY 9: Personal data of a third party withheld from an access request made by the parent of a minor

We received a complaint from an individual who had submitted an access request to a sports club for the personal data of their minor child, for whom the parent was the joint legal guardian. Following intervention from this office, the complainant had received personal data relating to their child from the sports club which was contained in an application for membership of the sports club which had been submitted to the sports club on behalf of the child. However certain information had been redacted from that application form, namely the names of the persons who were submitted to the sports club as emergency contacts for the child, the signature of the person who consented to images of the child being used on digital media by the sports club and the address of the minor. The complainant asserted that the third-party details and the address were all the personal data of their child and that the complainant as the joint legal guardian was therefore entitled to access to it. The sports club's position was that there was no express provision within Section 4 of the Data Protection Acts 1988 and 2003 (the Acts) which relates to the right of access, which allows a person access to another party's personal data without their consent. The sports club had also checked with the third parties whose personal data was the subject of the redactions on the application form as to whether they consented to the release of the data to the complainant but they had refused to give their consent.

Section 4(4) of Acts which precludes the release of third party data without that party's consent was brought to the attention of the complainant. However, the complainant put forward the argument that because the information requested pertained to matters concerning the minor's welfare and that because the third party was the legal representative of that minor, this rendered the data to be the child's personal data. We outlined the definition of personal data to the complainant and highlighted case law which has established that a individual's name represents the personal data of that individual. The complainant was also advised that the address of their child could not be provided without also providing the personal data of a third party and therefore the complainant had no right of access to it.

The complainant sought a decision on their complaint from the Commissioner. In her decision, the Commissioner pointed out that taking account of Section 8(h)

of the Acts (which lifts restrictions on the processing of personal data where the processing is made with the consent of the data subject or a person acting on their behalf), her office's position is that a parent or legal guardian of a young child has an entitlement to exercise the right of access on that child's behalf. However, in this case as the child in question could not be identified by the names of third parties who were listed as emergency contacts with the sports club, the information to which the complainant sought access was not the personal data of the complainant's child. The Commissioner in her decision pointed out that if the complainant's logic were to be followed and an emergency contact were deemed the personal data of a third party, an adult who has listed another adult as an emergency contact would have the right of access over that third party' name, telephone number, address, etc. The Commissioner found that no contravention of the Acts had occurred in relation to the redactions made to documents which had been released by the sports club on foot of the access request.

This case illustrates that irrespective of the relationship, dependency or connection between two parties, the name of a third party cannot be deemed to be the personal data of a data subject. As highlighted in the Commissioner's decision, to do so would deprive that third party of control over their own personal data and allow another individual to exercise data subject rights, including the right of access, over the personal data of the third party. Such an outcome would run contrary to the core principle of data protection which is that each data subject has the right to determine the use of their own personal data. However, it is important to distinguish this principle from the limited circumstances in which *the rights* of a data subject may be lawfully *exercised* by another person who is permitted to do so on their behalf. Even where data subject rights may be exercised by a third party (such as the parent of a young minor child) this does not render the personal data of the data subject to be the personal data of the third party who is authorised to exercise the data subject's rights on their behalf.

CASE STUDY 10: Disclosure of Personal Data via a Social Media App

We received complaints from two individuals who each claimed that their personal data had been unlawfully disclosed when it was broadcast on "Snapchat", an instant messaging and multimedia mobile application.

The complainants, who were friends, informed us that they had each submitted their CV with a cover letter to a particular retailer, in person, by way of application for employment with that retailer. The applications had been made by the complainants on the same day and had been received by the same employee of the retailer. Later on the same day the complainants had learned from a third party that a photograph showing both cover letters was appearing on "Snapchat" with a message drawing attention to similarities in the cover letters. It was the complainants' common understanding that the employee of the retailer to whom they had submitted their CVs had taken this photograph and posted it to "Snapchat".

During the course of our investigation of these complaints, we established that the employee of the retailer to whom the complainants had handed their CVs and cover letters had been recently notified by the retailer of the termination of their employment. Contrary to the retailer's policy and the terms of their contract of employment, the employee had a mobile phone on their person during work hours and had used it to take a photograph of both the cover letters and to post it to "Snapchat". The retailer informed our investigators that the employee was aware that this action was contrary to their contract of employment and the actions of the employee were done in circumstances where the employee was about to leave their employment. The retailer insisted that, in this instance, there was nothing further it could have done to prevent this incident from occurring.

In her decision the Commissioner found that the retailer, as the data controller for the complainants' personal data, had contravened Section 2A(1) of the Data Protection Acts 1988 and 2003 as the processing of the complainants' personal data, by way of the taking and posting of the photograph by the retailer's employee, was incompatible with the purposes for which it had been provided to the retailer by the complainants.

The case should serve as a cautionary reminder to data controllers that as a general principle under data protection law, they are responsible for the actions of their employees in connection with the processing of personal

data for which they are the data controller. The motive of an employee or the deliberate or accidental nature of the actions which they have undertaken in relation to personal data does not absolve data controllers of such responsibility. Data controllers have an obligation to ensure that their employees comply with data protection law in relation to the personal data which they hold irrespective of whether it is the employee's first or last day or employment with the data controller. Indeed this obligation will continue even after an employee leaves a data controller's employment if that employee can still access the personal data controlled by their former employer.

CASE STUDY 11: Failure by the Department of Justice and Equality to impose the correct access restrictions on access to medical data of an employee

We received a complaint from an individual concerning an alleged disclosure of their sensitive personal data by the Department of Justice & Equality (the Department). It was claimed by the complainant, who was an employee of the Department, that a report containing information on the complainant's health had been uploaded to a general departmental open document management database in 2012 and that the report had remained on that database for up to three years where it could be accessed by approximately 80 employees. The complainant informed us that they had been notified of the accessibility of the report on the database by a colleague. The complainant told us that they had requested an explanation from the Department as to why the report had been placed on an open database but had not received official confirmation that the report had since been removed.

We commenced an investigation into the complaint. The Department confirmed that notes relating to a discussion which had taken place between the complainant and their line manager in 2012 (which included a note concerning the complainant's health) had been stored to the database in question and marked private. However, the line manager had inadvertently omitted to restrict access to the document with the result that it could be accessed by approximately 80 staff members from the Department. The Department informed us that the document had been removed from the database in question some 3 years after having been saved to it. As the line manager in question had since left the Department, it had been unable to establish exactly why the document had been saved there in the first place but claimed that it was due to human error. The Department was also unable to establish how many staff had actually accessed the document during the 3 year period in which it was accessible as the Department's IT section had been unable to restore the historic data in question.

The Department made an offer, by way of amicable resolution, to write to the complainant confirming that the document in question had been removed from the database and apologising for any distress caused. The complainant chose not to accept this offer and instead sought a formal decision of the Commissioner. In her decision, the Commissioner concluded that the Department had contravened Section 2A(1) and 2B(1) of the Data Protection Acts 1988 & 2003 by processing the complainant's sensitive personal data without the required consent or another valid legal basis for doing so and by disclosing the complainant's sensitive personal data to at least one third party. These contraventions had occurred by way of the placing of a confidential document containing details of the complainant's health on an open database where it appeared to have remained accessible for 3 years and had been accessed by at least one co-worker.

This case is a stark illustration of the consequences for a data subject and general distress which can be caused where the data controller fails to ensure that its staff have adhered to, and continue, to adhere to proper document management protocols for documents containing personal data and moreover, sensitive personal data. While the controller in question was unable to identify how many times and by how many different staff members the document in question had been accessed during the 3 year period when it was accessible to approximately 80 staff members, the potential for further and continuing interference with the data subject's fundamental rights and freedom remained throughout this period. Had the controller in this case had adequate regular audit and review measures in place for evaluating the appropriateness of documents stored to open access databases, the presence of this confidential document would have been detected much sooner than actually occurred. Further, had the Department an adequate system of training and ensuring awareness by staff managers of basic data protection rules in place, this issue may not have arisen in the first instance.

Prosecutions Unit: Marketing Offences

CASE STUDY 12: Virgin Media Ireland Limited

We received a complaint in May 2016 from an individual who had received unsolicited marketing telephone calls from Virgin Media Ireland Limited in March and in May 2016 after she had previously asked the company not to call her again. The complainant is a customer of Virgin Media Ireland Limited and she informed us that the calls promoted Virgin Media products. She advised us that when the company first called her in January 2016 she had asked that her details be placed on the "Do Not Call" list as she did not wish to receive any further marketing calls. She stated that when the company called her again in March 2016 she repeated that she wanted her details to be placed on the "Do Not Call" list but despite her two requests she had received a further unsolicited marketing telephone call to her mobile phone on 27 May 2016.

During our investigation of this complaint, Virgin Media Ireland Limited informed us that due to human error the complainant's account was not updated correctly to record the "Do Not Call" requests. The company advised us that a review had been conducted on all "Do Not Call" requests handled by the team in question for the period from January 2016 to July 2016 to ensure that all opt-out requests had been completed correctly. It confirmed that the complainant's details had been removed from the marketing database and it apologised for any inconvenience caused to her.

Prior to September 2015 Virgin Media Ireland Limited traded under the name UPC Communications Ireland Limited. That company had previously been prosecuted, convicted and fined in March 2011 and in April 2010 for twenty similar marketing offences involving telephone calls to subscribers who had not consented to the receipt of such marketing calls. The Data Protection Commissioner therefore decided to prosecute Virgin Media Ireland Limited in respect of the offences identified following the investigation of the latest complaint.

At Dublin Metropolitan District Court on 3 July 2017, Virgin Media Ireland Limited pleaded guilty to two charges of making unsolicited marketing telephone calls to its customer after she notified the company that she did not wish to receive such calls. The Court convicted the company on both charges and it imposed fines of €1,500 and €1,000 respectively on the charges. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

CASE STUDY 13: Sheldon Investments Limited (trading as River Medical)

In September 2015 we received a complaint against Sheldon Investments Limited, trading as River Medical, from an individual who had received unsolicited marketing emails to which he had not consented and which were subsequent to his attempts to opt out of such emails. In making his complaint, the individual explained that he had previously had a consultation with River Medical during which he was obliged to complete a form. He stated that when completing the form he expressly stated that he did not wish to receive any marketing emails from them. He subsequently received a marketing email from River Medical in April 2015 and he replied to the email with a request that his address be removed from their marketing list immediately. He received confirmation two days later that his contact details were removed. Despite this, he received a further unsolicited marketing email from River Medical in September 2015 which prompted him to submit a complaint to the Data Protection Commissioner.

During our investigation of this complaint, River Medical told us that the failure to respect the complainant's opt-out request was due to human error. It explained that it had made his file 'inactive' on receipt of his opt-out request, but it did not realise that it needed to manually delete his file in order to prohibit the sending of further marketing material to him. It assured us that on foot of our investigation of the complaint, the individual's email address had been deleted from its systems. We concluded the investigation of that complaint in December 2015 with a warning to the company that it would likely be prosecuted if it committed any further offences under the marketing regulations.

One year later, in December 2016, the individual submitted a new complaint after he received a further unsolicited marketing email from River Medical. We investigated this complaint and we were informed once again that the latest infringement had been caused by human error in the selection of an incorrect mailing list on Newsweaver, the system used by the company to issue emails. The company apologised for the incident.

As we had previously issued a warning to the company, the Data Protection Commissioner decided to prosecute it in respect of the two unsolicited marketing emails issued in December 2016 and in September 2015. At Dublin Metropolitan District Court on 3 July 2017, Sheldon Investments Ireland Limited pleaded guilty to

two charges of sending unsolicited marketing emails without consent. The Court sought the payment of €800 in the form of a charitable donation to Focus Ireland and it adjourned the matter. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner. At the adjourned hearing the defendant produced proof of payment of the charitable donation and the Court struck out the charges.

CASE STUDY 14: Tumsteed Unlimited Company (trading as EZ Living Furniture)

In June 2016 we received a complaint from an individual who received unsolicited marketing text messages from EZ Living Furniture despite having, on three previous occasions, requested them to stop. The complainant informed us that she had made a purchase from the company in the past.

As part of our investigation of this complaint, we asked EZ Living Furniture to show us evidence of the consent of the complainant to receive marketing text messages in the first instance. We also sought an explanation as to why her requests to opt out had not been actioned.

In response to our investigation, EZ Living Furniture stated that, in respect of marketing consent, customers sign into the company's terms and conditions printed on the back of receipts. It drew our attention to one of the terms and conditions to the effect that customer information will be retained by the EZ Living marketing department and will be added to its database to be used for mailing lists and text messages. In relation to the complainant's opt out requests not being complied with, EZ Living Furniture explained that there had been a changeover of service providers and the new service provider had a different method for opting out. It claimed that it was totally unaware that the opt-out facility was not working until it received our investigation letter. It assured us that the opt-out issue had now been resolved and it said that it had sent an apology to the complainant. In our response to EZ Living Furniture, we advised it, in relation to customer consent, that while it was relying on terms and conditions of sale, it was in fact obliged by law to provide its customers with an opportunity to opt out of receiving marketing communications at the point of collection of their personal data. We pointed out that, in practice, this means that customers must be provided with an opt-out box for them to tick in order to opt out of marketing, if that is their wish. In a subsequent reply, the company informed us that it had examined the matter further and that it had decided to introduce a stamp that would be placed on the sales docket to provide a checkbox to allow customers to opt out of receiving marketing emails and text messages.

The Data Protection Commissioner had previously issued a warning to EZ Living Furniture in April 2015 following the investigation of a complaint from a different individual in relation to sending her unsolicited marketing text messages without consent. Consequently, the Data Protection Commissioner decided to prosecute the company in respect of the offences which came to light arising from the latest complaint.

At Galway District Court on 4 July 2017, Tumsteed Unlimited Company, trading as EZ Living Furniture, pleaded guilty to two charges of sending unsolicited marketing text messages without consent. The Court convicted the company and it imposed fines of €500 on each of the two charges. The company agreed to make a contribution towards the prosecution costs of the Data Protection Commissioner.

CASE STUDY 15: Cunniffe Electric Limited

In December 2016 an individual complained to us that he had recently received unsolicited marketing text messages from Cunniffe Electric Limited of Galway Shopping Centre despite the fact that he had been advised previously on foot of an earlier complaint to us that his mobile phone number had been removed from its marketing database. In early 2015 we had received the complainant's first complaint in which he informed us that he had given his mobile phone number some years ago to Cunniffe Electric Limited to facilitate the delivery of an electrical appliance which he had purchased from the company. He stated that he did not give the company consent to use his mobile phone number for marketing purposes.

Following our investigation of the first complaint, we received confirmation from Cunniffe Electric Limited that the complainant's mobile phone number had been removed from its marketing database. We concluded that complaint by issuing a warning to the company that it would likely face prosecution if it breached the marketing regulations again.

On receipt of the complainant's second complaint, we commenced a new investigation in which we sought from Cunniffe Electric Limited an explanation for the sending of the latest marketing text messages in circumstances

where we were previously informed that the complainant's mobile phone number had been removed from its marketing database. In response, the company admitted that it did not have the consent of the complainant to send him marketing text messages. It said that his mobile number was not on its database but it appeared that there was an error on the part of the service provider that it was using to send marketing text messages and that this error arose from transition issues when the service provider was acquired by another company. It apologised for the inconvenience caused to the complainant.

As the company had previously received a warning, the Data Protection Commissioner decided to prosecute it in relation to the most recent offences. At Galway District Court on 4 July 2017, Cunniffe Electric Limited entered a guilty plea for the sending of an unsolicited marketing text message without consent. In lieu of a conviction and fine, the Court asked the company to make a contribution of €500 to the Court Poor Box and it then struck out the charges. The company agreed to make a contribution towards the prosecution costs of the Data Protection Commissioner.

CASE STUDY 16: Argos Distributors (Ireland) Limited

Five individuals lodged complaints with us between December 2016 and February 2017 arising from difficulties they were experiencing in opting out of email marketing communications from Argos Distributors (Ireland) Limited. The complainants had supplied their email addresses in the context of making online purchases and they had not opted out of marketing communications at that point. However, when they subsequently attempted to opt out on receipt of marketing emails, the 'unsubscribe' system failed. Some complainants subsequently followed up by email to the company seeking to have their email addresses removed from the marketing database and they received responses by email to inform them that their requests had been actioned. However, they continued to receive further email marketing from Argos Distributors (Ireland) Limited.

In response to our investigation, the company acknowledged that its 'unsubscribe' system was not working properly for a period of time. It also discovered an issue in processing 'unsubscribe' requests for customers based in Ireland. It found that requests from Irish customers were being added to the 'unsubscribe' list for UK marketing. In all cases, it confirmed that the opt-out requests of the individuals concerned were now properly processed.

As the company had been warned previously in 2013 following the investigation of a similar complaint of a breach of the marketing regulations, the Data Protection Commissioner decided to prosecute it in relation to these offences. At Navan District Court on 14 July 2017, Argos Distributors (Ireland) Limited pleaded guilty to five charges of sending unsolicited marketing emails to five individuals without consent. In lieu of a conviction and fine, the Court ordered the defendant to contribute €5,000 to a charity of the Court's choosing. The defendant agreed to pay the prosecution costs incurred by the Data Protection Commissioner.

CASE STUDY 17: Expert Ireland Retail Limited

In October 2016 an individual complained to us about regular marketing text messages which she received from Expert Ireland Retail Limited. She informed us that in August 2014 she purchased a tumble dryer at the Expert Naas store and she stated that she gave her mobile phone number at the point of sale for the sole purpose of arranging the delivery of the appliance. She stated that she was not asked if she wished to receive marketing text messages and she did not request or agree to same. She informed us that she began receiving regular marketing text messages from December 2015 onwards and despite replying by text message on numerous occasions with the opt-out keyword, further text messages continued to arrive on her phone. She advised us that early in October 2016 her husband called to the Expert store in Naas and he asked the staff there to remove her number from their marketing database. Despite this request the complainant received a further marketing text message about two weeks later, prompting her to lodge a complaint with the Data Protection Commissioner.

In response to our investigation, the company claimed that the complainant would have been asked during the course of the sale if they would like to be contacted by text message for marketing purposes. However, it was unable to provide any evidence that the complainant was given an opportunity to opt out of marketing at the point of sale. Furthermore, it admitted that the sending of the first marketing message after a period of over twelve months had expired was an oversight. The company was

unable to explain why no action was taken to remove the complainant's mobile phone number from the marketing database after her husband called to the Naas store.

As the company had previously been issued with a warning in May 2010 on foot of a similar complaint which we received about unsolicited marketing text messages sent to a different former customer of the Expert store in Naas without her consent, the Data Protection Commissioner decided to prosecute this latest complaint. At Mullingar District Court on 13 October 2017, Expert Ireland Retail Limited pleaded guilty to one charge of sending an unsolicited marketing text message to the complainant without her consent. The Court convicted the company and it imposed a fine of €500. The defendant company agreed to pay the legal costs incurred by the Data Protection Commissioner in respect of this prosecution.

Appendix III

Data protection case law of the CJEU

There were a number of significant judgments delivered by the CJEU during 2017 which concerned the interpretation of EU law as it relates to data protection. The Commissioner was a party to one of these cases *(Nowak v. Data Protection Commissioner)*. The key aspects of these judgments, insofar they relate to issues of data protection, are summarised below.

Peter Nowak v Data Protection Commissioner Case C-434/16 *(Judgment of the Court, Second Chamber, delivered on 20 December 2017)*

This case involved a request for a preliminary ruling, by the Irish Supreme Court, on the issue of whether the written answers contained in the examination script of a candidate in a professional examination, and the examiner's comments on those answers, constitutes personal data, within the meaning of the 1995 Data Protection Directive.

Mr. Nowak, a trainee accountant, 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 (then) 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. Mr Nowak appealed this 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 ultimately held that there was a right to appeal against a decision of the Commissioner not to investigate a complaint. On the question of whether the examination script in question constituted personal data, the Supreme Court referred the issue to the CJEU.

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.

In relation to the examination answers, the Court held that the content of answers in a professional examination reflect (i) a candidate's knowledge and competence in a given field (ii) in some cases his intellect, thought processes and judgment; and (iii) in the case of handwritten examinations, information as to the candidates' handwriting. The Court also considered it relevant that the purpose of the collection of this data is to assess the candidates' suitability to practice the profession concerned and that the use of the information (i.e. to assess whether the candidate had passed or failed) could affect a candidate's rights and interests with regard to their chances of entering the profession or obtaining a post.

In relation to the examiner's comments, the CJEU ruled that these reflected the opinion/ assessment by the examiner of the candidate's performance in the examination, their purpose was to record that evaluation and they could have effects on the candidate's rights and interests. However, while noting that rights of access and rectification therefore applied to the answers submitted by a candidate at a professional examination, the Court pointed out that the right of rectification could not enable a candidate to "correct" answers that are "incorrect" and that such errors in answers do not represent inaccuracy within the meaning of the Data Protection Directive which would give rise to the right of rectification. However, the Court pointed to situations when the examiner's comments on the candidate's answers were inaccurate (therefore giving rise to the right of rectification), for example where examination scripts were mixed up so that answers of one candidate were ascribed to another or some of the cover sheets containing answers were lost so that the answers were incomplete or the comments of the examiner did not accurately record the examiner's evaluation of the candidate's answers.

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA 'Rīgas satiksme' — Case C-13/16 *(Judgment of the Court, Second Chamber, delivered on 4 May 2017)*

This case involved a request for a preliminary ruling, by the Latvian Supreme Court, on the interpretation of processing *'necessary for the purposes of the legitimate interests'* (Article 7(f) of the 1995 Data Protection Directive. The CJEU was asked to determine whether the 'legitimate interests' ground must be interpreted as imposing *an obligation* to disclose personal data to a third party in order to enable an action for damages to be brought before a civil court.

The facts of the case involved a passenger (a minor) in the back seat of a taxi opening the taxi door just as a trolleybus was passing alongside the taxi, causing caused

damage to the trolleybus. The trolleybus company sought the passengers' details from the Latvian police (who had imposed an administrative penalty on the passenger in relation to the incident) for the purposes of suing the passenger for the damage caused. The Latvian police provided only the first and surname of the passenger and refused to provide any other information. The trolleybus company challenged this refusal in the Latvian Courts, which was appealed to the Supreme Court with a reference being made to the CJEU. The CJEU held that Article 7(f) of the 1995 Data Protection Directive does not impose an obligation to process data for 'legitimate interests' but rather allows for the possibility of processing data for this purpose. Further, the CJEU held that a disclosure of personal data under this legal basis is not precluded where it is made in accordance with national law and where it satisfies three cumulative conditions:

1. There is a **legitimate interest** pursued by the data controller or by the third party or parties to whom the data are disclosed;
2. There is a **need to process** personal data for the purposes of the legitimate interests pursued; and
3. That the fundamental rights and freedoms of the person of the data subject **do not take precedence**.

The CJEU ruled that there was no question but that the interest of a party in obtaining the personal information of a third party who has damaged their property for the purposes of suing them qualifies as a legitimate interest. Insofar as the balancing of rights and interests was at issue under this provision of the 1995 Data Protection Directive, the age of the data subject may be one of the factors which is taken into consideration in balancing these rights and interests. On this issue, the CJEU indicated (but made it clear that this issue was subject to the Latvian Court's own determination) that the fact that the data subject in question here was a minor was justification to refuse to disclose data identifying the data subject (or the person with parent responsibility for that data subject) for the purposes of bringing an action for damages against the data subject.

Camera di Commercio, Industria, Artigianoto e Agricoltura di Lecce v Salvatore Manni — Case C-398/15 *(Judgment of the Court, Second Chamber, delivered on 9 March 2017)*

This case involved a request for a preliminary ruling, by the Court of Cassation, Italy, as to whether Member States must allow individuals to have public access to personal data relating to them, contained in the national companies register, limited on a case-by-case assessment when the company in question had been dissolved.

Mr. Manni had been the sole director of a company which had been declared insolvent in 1992 and was struck off the Italian companies register in 2005. That information was accessible to the public on the companies register. Mr Manni had objected to the inclusion of that information on the companies register and had sought an order that the data linking him to the company which had been struck off be erased, anonymised or blocked as he claimed that the presence of that information on the companies register was having adverse effects on his current business pursuits.

In its judgment, the CJEU considered the purpose of disclosing such information on a companies register, which it said was legal certainty and to protect the interests of third parties and it was important that third parties were able to establish essential information about the constitution of companies with which they wished to trade and about the parties authorised to bind those companies. It also noted that such company information contains only limited personal data items, i.e. relating to the identity and the respective functions of the person authorised to bind the company. For these reasons the CJEU considered that this information should be disclosed so third parties can see their content. The CJEU noted that even after dissolution of a company certain legal rights and relations remain e.g. to bring actions against the members or liquidators or a company. However, in light of the various legal rights and differing limitation periods in Member States, it was impossible to identify one defined time limit following the date of dissolution of a company after which the inclusion of such personal data in the companies register would not be necessary. The fact that Member States could not guarantee a right of erasure for personal data from the companies register following a certain period after dissolution of a company did not result in a disproportionate interference with the rights of the data subjects concerned, including the rights under Articles 7 and 8 of the Charter of Fundamental Rights of the EU.

It was for Member States to determine whether individuals could apply to the authority which keeps the companies register to limit access to personal data relating to them in the register to third parties who can show a particular interest in accessing the data. However, any limitation of access rights to such information kept on the companies register could only be determined on a case-by-case basis, and had to be exceptionally justified on compelling legitimate grounds following the expiry of a sufficiently long time after the dissolution of the company.

Peter Puškár v Finančné riaditeľstvo Slovenskej republiky and Kriminálny úrad finančnej správy Case C-73/16 *(Judgment of the Court, Second Chamber, delivered on 27 September 2017)*

This case involved a request for a preliminary ruling by the Slovakian Supreme Court on, among other matters, the interpretation of *'necessary for the performance of a task carried out in the public interest'* (Article 7(e), Directive 95/46/EU).

Mr. Puškár claimed his rights were infringed by the inclusion of his name on a list of persons acting as 'fronts' in company director roles (called the 'contested list') which was drawn up by a tax authority for the purpose of collecting tax and combating tax fraud. The existence of the contested list was not disputed by the tax authority in question. The CJEU considered that the fact of a person being included on the contested list is likely to infringe some of their rights — for example, it could affect the presumption of innocence of that person and affect the freedom of enterprise of companies associated with the people on the list. However, the processing of personal data by Member State authorities by the drawing up of a "contested list" without the consent of the data subjects, for the purpose of collecting tax and combating tax fraud was not precluded by EU law provided the following conditions are met:

- that those authorities are required by national legislation to carry out this task in the public interest;
- that drawing up of the list is appropriate and necessary to achieve the objectives pursued;
- that there are sufficient indications to assume that the data subjects' names are properly included in the list; and
- all of the conditions of lawfulness of processing, as per the Data Protection Directive are satisfied.

Transfer of Passenger Name Record ['PNR'] data from the European Union to Canada, Opinion pursuant to Article 218(11) TFEU on the draft Agreement between Canada and the European Union *(Opinion 1/15 of the Court, Grand Chamber, delivered on 26 July 2017)*

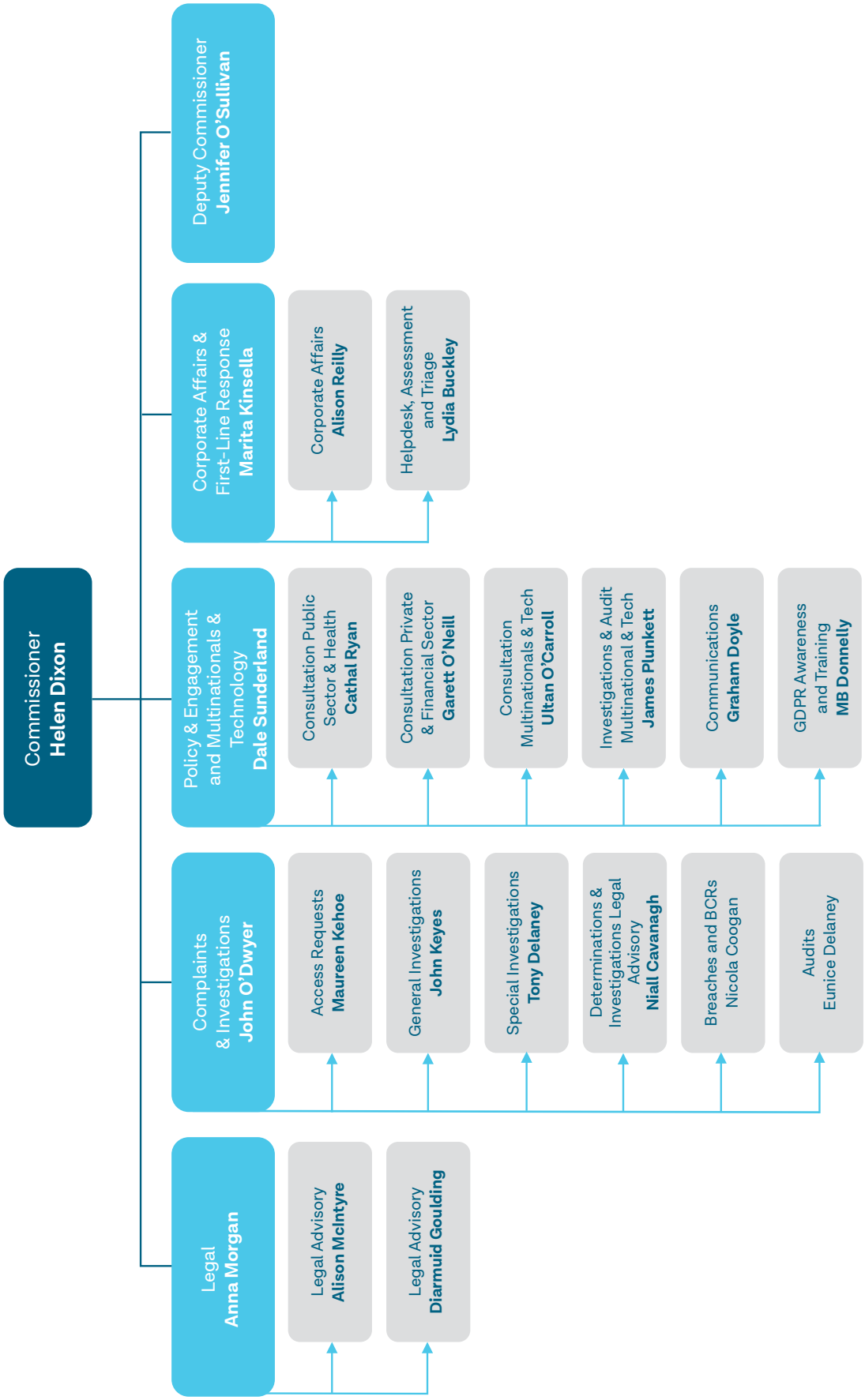
For the first time, the CJEU was required to rule on the compatibility of a draft international agreement with the Charter of Fundamental Rights of the European Union (**the Charter**), particularly Article 7 (respect for private and family life) and Article 8 (the protection of personal data).

An agreement on the transfer and processing of PNR data was negotiated between the EU and Canada and signed in 2014 (the **PNR Agreement**). The PNR agreement envisaged the transfer of PNR data of passengers carried by airlines flying between the EU and Canada, to Canadian public authorities for the purposes of combatting terrorism and other serious transnational crime, while providing guarantees in relation to the protection of passengers' personal data and privacy. The European Parliament was asked, by the Council of the European Union, to approve the PNR Agreement and the European Parliament in turn asked the CJEU to deliver an Opinion on the compatibility of the PNR Agreement with EU law.

The CJEU held that under EU law, the PNR agreement could not be concluded in its current form as several of its provisions were incompatible with the fundamental rights recognised by EU law. The CJEU ruled that while the interference with the fundamental rights to respect for private life and protection of one's personal data in certain provisions was justified by the pursuit of the objective of securing public security in the fight against terrorism and serious transnational crime, these interferences went beyond what was strictly necessary for the pursuit of that objective. In respect of other provisions (namely the envisaged transfer of sensitive personal data) the interference with the fundamental rights was not justified. The CJEU pointed to a range of provisions which it said, were incompatible with fundamental rights unless the agreement was revised in order to better delimit and refine the interferences with the fundamental rights.

Appendix IV

Organisation Chart



Organisation Chart as of February 2018

Appendix V

Statement of Internal Controls

Scope of Responsibility

On behalf 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 Office of the Data Protection Commissioner for the year ended 31 December 2017 and up to the date of approval of the financial statements.

Capacity to Handle Risk

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 5 times in 2017. The Office of the Data Protection Commissioner's senior management team acts as the Risk Committee for the body. Senior managers from the Office of the Data Protection Commissioner 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 carry 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 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 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 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 Data Protection Commissioner with ICT services. They have provided an assurance statement outlining the control processes in place in 2017 in respect of the controls in place;

- there are systems in place to safeguard 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 Data Protection Commissioner has procedures in place to ensure compliance with current procurement rules and guidelines and that during 2017 the Office of the Data Protection Commissioner complied with those procedures.

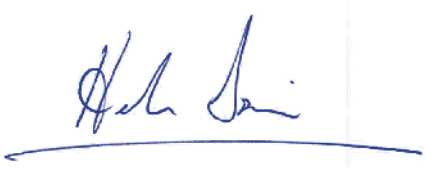
Review of Effectiveness

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 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, and the senior management team. The senior management within the Data Protection Commissioner is responsible for the development and maintenance of the internal financial control framework.

I confirm that the Data Protection Commissioner conducted an annual review of the effectiveness of the internal controls for 2017. It should be noted that this extended beyond financial controls and examined ICT controls, management practices and other governance processes.

Internal Control Issues

No weaknesses in internal control were identified in relation to 2017 that require disclosure in the financial statements.



Helen Dixon
Data Protection Commissioner

Appendix VI

Energy Report

Overview of Energy Usage in 2017

Dublin — 21 Fitzwilliam Square

The Dublin premises of the office of the Data Protection Commissioner is based in 21 Fitzwilliam Square, Dublin 2. By the end of 2017 there were approximately 40 people accommodated in this building. In 2017 the sources of the main usage of energy in the Office was electricity for heating, lighting and other uses.

The Dublin premises at 21 Fitzwilliam Square is a protected building, and therefore exempt from the energy rating system.

Portarlington

The DPC's Portarlington office is located on the upper floor of a two-storey building built in 2006 with a floor area of 444 square metres. At end 2017, 28 members of staff were accommodated in this building. In 2017, the main use of energy in the Office was for gas and electricity for heating, lighting and other uses.

In 2017 the energy rating for the building in Portarlington was C1.

Dublin — Regus Building

In August 2017, the DPC took out a short-term office agreement for additional space in the Regus Building, Harcourt Road, Dublin 2 to accommodate the increase in staff resources. By the end of 2017 there were 14 people accommodated in this building as an interim arrangement pending the finalisation of a larger Dublin premises to accommodate all DPC-based staff. The DPC's energy usage for this building is not available.

Actions Undertaken

The DPC has participated in the SEAI online system in 2017 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 annual energy usage for the office for 2017:

Dublin office

Usage	
Usage	
Non-electrical	N/A
Electrical	77,240 kWh

Portarlington office

Usage	
Usage	
Non-electrical	45,203 kWh
Electrical	29,850 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

The 2017 Account of Income and Expenditure is currently being prepared and will be submitted to the Comptroller & Auditor General for audit. Once the audit is concluded the 2017 Financial Accounts will be appended to this report.

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner