

20

16

**Annual Report of the
Data Protection Commissioner of Ireland**



**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

| | |
|--|----|
| Foreword: Annual Report 2016 | 1 |
| Role and Responsibilities of the Data Protection Commissioner of Ireland | 5 |
| Review of 2016 in Brief | 8 |
| Contacts, Queries and Complaints | 10 |
| Special Investigations | 12 |
| Data Breach Notifications | 14 |
| Multinationals and Technology | 17 |
| Consultation | 21 |
| Privacy Audits | 23 |
| Legal | 27 |
| Binding Corporate Rules and Google Common Position Application | 34 |
| Guidance and Outreach | 35 |
| EU and International Engagement | 37 |
| Registration | 39 |
| Corporate Affairs | 40 |
| Appendix 1 - List of Organisations Audited or Inspected in 2016 | 46 |
| Appendix 2 - Case Studies | 47 |
| Appendix 3 - Data-protection Case Law of the CJEU | 55 |
| Appendix 4 - Organisation Chart | 56 |
| Appendix 5 - Account of Income and Expenditure | 57 |
| Appendix 6 - Energy Report | 58 |



Anna Morgan, John O'Dwyer, Helen Dixon, Dale Sunderland, Jennifer O'Sullivan

Foreword Annual Report 2016



Ms. Helen Dixon
Data Protection
Commissioner

I'm very pleased to present the 2016 Annual Report of the Data Protection Commissioner (DPC), highlighting key developments and the activities of the Office for last year, together with the priorities for 2017 and beyond. 2016 was memorable as an Olympic year in the world of sports and it could be said that it was truly an Olympic year in the data-protection sphere too.

Big Strides Forward in Europe

We finally arrived at the enactment of the General Data Protection Regulation (GDPR) in May. This came four years after the publication of the EU Commission proposal of 2012 aimed at modernising and updating Europe's framework law safeguarding the right to protection of personal data under the EU Charter of Fundamental Rights. Critically, this new law promises a significantly greater ability for each of us to more effectively control and understand the uses of our personal data in this Big Data era. Equally, we saw a further seminal ruling from the Court of Justice of the European Union (CJEU) in the *Tele2 Sverige* and *Watson* joint case, where the court further clarified the necessity and proportionality test set out in its *Digital Rights Ireland* judgment of 2014 and specifically laid down that Member States may not impose a general, non-targeted obligation to retain data on providers of electronic communications services. The Privacy Shield also entered the stage in the summer of 2016 after it was agreed between US authorities and the EU Commission as a lawful basis for qualifying companies to transfer personal data from the EU to the US in the wake of the strike-down of *Safe Harbour* by the CJEU in October 2015.

Internet Companies to the Fore

In Europe, big internet companies became an unsurprising focus of media attention as company mergers and mass-scale data breaches came to the fore. The Facebook and WhatsApp merger clearly demonstrated the complexities of disentangling the data-protection element from broader consumer interests in this type of scenario. Many debate whether 'take it or leave it' user policies, where the only means of avoiding data being shared between two merging entities is to exit and discontinue use of the service completely, are wrong, unlawful or both. From a data-protection point of view, it's not clear that such a policy would be automatically prohibited – if a user freely gives consent, having been adequately put on notice about what personal data is in scope and in what relation it will be used, then such sharing can be legitimised purely from a data-protection point of view. But there are, perhaps, as some argue, other ways in which the trade of paying with personal data is unfair to consumers, notwithstanding that the services are free-of-charge in a monetary sense.

For this reason, the Irish DPC commends the fledgling initiative of the European Data Protection Supervisor in 2016 to establish a Digital Clearing House that will bring together, on a voluntary basis, data-protection authorities and consumer and competition regulators to look at ways in which cooperation between the different authorities can lead to web-based service providers being more accountable for their conduct. It's clear that power in terms of internet tracking and driving profit from interest-based ads lies largely in the hands of a few big platforms and that questions need to be asked and answered as to whether consumers are being left between a rock and a hard place with too little choice (and therefore subject to a type of 'forced consent') given that media outlets are all signed up to those same ad exchanges. Again, I believe this is not purely a data-protection issue but rather one that needs coordinated action by the various regulators in the consumer space. If all users can and do opt out of online tracking for advertising purposes and, as a result, online content must be accessed from behind a paywall, does this improve the overall rights of consumers? Similarly, can businesses be forced to offer both free and paywalled services? The EU Commission's draft ePrivacy Regulation, published in January 2017, is an interesting input to this space, with some arguing that its absolute emphasis on consent when accessing a user's device (i.e. reading a mobile device or dropping a cookie onto a desktop device) will only centralise more power in the hands of the few biggest ad exchanges and ultimately deliver no real improvement to the lot of the consumer.

The long-awaited ruling in the summer of 2016 from the Second Circuit in the US in the Microsoft warrant case further underlined the complexity of applying jurisdictional laws to the global internet. The court decided that Microsoft was not required to hand over emails located on a server in Ireland to a law-enforcement agency in the US pursuing the investigation and prosecution of drugs offences. While many hailed the outcome as a victory for data privacy rights, others equally concerned with those rights suggested that the emphasis on physical server location could deliver an opposite outcome depending on the location of the physical server.

The massive data breaches suffered by Yahoo! also provided a salutary reminder of the sheer quantity of our personal data stored by online service providers. For the European controllers of US internet companies that transfer data to the US for further processing, clear obligations exist under Irish law requiring the Irish-based controllers to ensure that the data is adequately safeguarded by the processor. This process of ensuring adequate controls must be an active and ongoing one that continues to be implemented long after the controller-to-processor agreement is signed and put in the drawer. While in some cases it may be impossible to adequately safeguard against particularly sophisticated criminal hacking, with proper monitoring, audits and controls, in many circumstances the existence of a breach of systems may be identified much sooner and mitigation action taken.

Continued Expansion of DPC

For the Irish DPC, 2016 has been another year of building, expanding, upskilling and driving better response times in our work. Close to 70 staff are now on board following a year of strong targeted recruitment that delivered industry-expert legal practitioners, technologists and project managers. The expanded senior level of the DPC organisation is now in a position to drive forward and deliver on our evolving and expanding regulatory role under the GDPR. These preparations include a new additional round of substantial recruitment, with 35 staff to be added in 2017, including further legal, investigative, business analysis, and content/copywriting specialists.

In 2016, the DPC finally launched a Twitter presence and the account is now among the fastest growing of the International Conference of Data Protection Commissioners! Pushing out guidance to organisations on GDPR is a key priority and the DPC in 2016 commenced its roll-out with an active programme planned for 2017. The implementation of a harmonised law across Europe means that work has been intense within the Article 29 Working Party of EU Data Protection Authorities in 2016 as we seek to ensure a common view and issue guidance to industry on important new concepts such as data-protection officers, mandatory breach notifications and the one-stop shop. The DPC has also sought to ensure that government takes account of the DPC's on-the-ground regulatory experience in drafting the new Irish Data Protection bill to underpin GDPR implementation and, in particular, to ensure that, as the independent enforcer of data-protection law, we have a full range of powers available to us to deliver on our role.



An Taoiseach, Enda Kenny T.D., at the official opening of the DPC's Dublin office in Fitzwilliam Square, accompanied by Data Protection Commissioner Helen Dixon and Minister of State Dara Murphy T.D.

The new Dublin city-centre offices of the DPC (in addition to the Portllington premises) have proven extremely valuable for stakeholder engagement. We were very pleased to welcome An Taoiseach Enda Kenny TD (prime minister) to formally open our Dublin offices in January 2017 where he underlined his government's deep understanding of the importance of protecting personal data and its commitment to funding a strong, independent enforcement authority. Such is the rate of our recruitment programme that an additional nearby premises is now being sought by the DPC to house the further staff members who will join the DPC over the next two years, bringing our Dublin-based staff to around 130.

Complaints and Enforcement

On foot of a year of committed work in handling complaints about organisations from individuals during 2016, the DPC welcomes the greater enforcement focus of the GDPR as a means of driving improved standards of compliance with data-protection law over and above what we see today. In 2016, the Irish DPC investigated over 1,400 individual complaints. Disappointingly, compliance with individuals' access rights to their personal data remains low and, accordingly, the DPC has recently run a targeted campaign highlighting organisations' obligations in this area. Other case studies demonstrate a failure by organisations to ensure that individuals are adequately on notice of how their data is being processed. Employee monitoring by means of CCTV remains a concern for many and, while in the case of some complaints the DPC investigated in 2016, it found that the monitoring and processing of CCTV images was lawfully justified, a trend emerges of employers failing to make the rules around reliance

on CCTV footage in disciplinary processes clear to employees. Disclosure of individuals' data to third parties arose in a number of cases where the front-line staff of certain public-sector bodies failed to respect that an individual's personal data should not automatically be given to their spouse or other family members on request. The right to data protection is a personal right regardless of marital or family status.

It was another busy enforcement year, with details of prosecutions set out in the sections on Special Investigations and Legal of this report.

On a more systemic scale, public-sector bodies and government departments are in many cases slow to adjust to the reality that data-protection rights cannot simply be legislated away without sufficient necessity and proportionality analysis and prejudice tests being applied. Ireland's surveillance and interception laws require a thorough modernisation both to bring them up to date to ensure that law-enforcement and intelligence agencies have state-of-the-art powers but also importantly to ensure that the rights of individuals are adequately protected, in particular through independent oversight of how these far-reaching powers are deployed. In mid-2016, the Tánaiste and Minister for Justice and Equality signalled that the law on investigatory powers in relation to electronic communications would be reviewed. The DPC would welcome an early output of this process. The DPC also appeared before the Oireachtas (Irish parliament) Health Committee in December 2016 to outline our concerns with the proposed role for the DPC in the Health Information and Patient Safety Bill, which it believes represents a very serious challenge to the required independence of the DPC. That serious matter aside,

The next 12 months are all about GDPR – both getting ready as an EU data-protection authority and helping organisations get prepared.

State bodies need to comprehend that the obligations in law, and the requirement to be accountable for their processing of personal data, rest with them and they cannot simply legislate to transfer their obligations to the independent regulator.

2016 did deliver some encouraging improvements in terms of DPC engagement with public-sector bodies such as those set out in the section on Consultation. On the other hand, ongoing leaking of data from government bodies to private investigators remains a challenge to be tackled; issues in relation to the processes and safeguards for handling sensitive files in certain State agencies are also under investigation by the DPC. Further, the audit of the civil service shared-services provider PeoplePoint demonstrated a concerning level of front-line human error in the handling of personal data and sensitive personal data in many cases, and the DPC intends to follow up on its audit recommendations during 2017. The implementation of large-scale government projects without specific legislative underpinning, but rather relying on generic provisions in various pieces of legislation, poses challenges in terms of the transparency to the public in relation to projects such as the Primary Online Database and the Public Services Cards and the uses to which personal data is now being applied.

While a lawful basis for such use of personal data can be cited, the need for notice and transparency is especially high in these types of cases and it is not always clear that public clarity has been delivered.

High Court Proceedings in Transfers Case

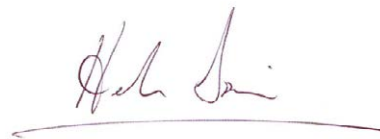
2016 was particularly noteworthy for the DPC in terms of the High Court proceedings launched in May seeking a reference to the CJEU to examine the validity of standard contractual clauses (SCCs) as a means of transferring EU personal data to the US. The 2017 hearing of the case in the Commercial Division of the Irish High Court ran for 21 days and shone a very bright spotlight on the considerable complexities of the laws and roles of the various actors relevant to this case (US and EU law; data-protection authorities, EU Commission, US government, US multinationals). Further details on this case are included in the Legal section of this report.

As further set out in the section on Legal, the DPC had a busy year in the courts, with an appeal against a decision in a ‘right to be forgotten’ case, judicial review proceedings concerning the DPC’s adjudicative powers, a Supreme Court ruling on appeal procedures and a reference to the CJEU on the scope of personal data relating to exam scripts. Furthermore, Digital Rights Ireland initiated a High Court action against the State alleging a lack of independence of the DPC, a position the DPC does not consider is sustained by the reality of our entirely independent regulatory operations.

Next 12 Months – It’s All About GDPR Readiness

The next 12 months are all about GDPR – both getting ready as an EU data-protection authority and helping organisations get prepared. GDPR readiness will also have to include taking account of the emerging implications of the UK’s exit from the EU. Significant efforts have been made during 2016 by the Irish DPC and these will continue in driving awareness of data-protection compliance issues for organisations. In this digital era, as technology hurtles forward, with artificial-intelligence applications including driverless cars already waiting just around the corner, it becomes ever more critical that the data-protection rights of individuals are vigorously defended. The GDPR provides a new and more robust platform from which the Irish DPC can pursue this objective.

Truly, a new era in data protection beckons ... we’re looking forward to it and we intend to be ready for it!



Ms. Helen Dixon
Data Protection Commissioner

Role and responsibilities of the Data Protection Commissioner of Ireland

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. Established in 1989, the power and authority of the DPC derives from the Data Protection Acts 1988 and 2003, which implemented the 1981 Council of Europe Data Protection Convention and the 1995 EU Data Protection Directive.

The main functions of the Office include investigations of complaints from individuals; identifying risks to personal data protection in a variety of public- and private-sector organisations through on-site inspections and audits; driving better compliance with data-protection legislation through the publication of high-quality guidance and regular and meaningful engagement with private- and public-sector organisations; and, ultimately, legal enforcement where necessary.

The main functions of the Office include investigations of complaints from individuals; identifying risks to personal data protection in a variety of public- and private-sector organisations through on-site inspections and audits; driving better compliance with data-protection legislation through the publication of high-quality guidance and regular and meaningful engagement with private- and public-sector organisations; and, ultimately, legal enforcement where necessary.

As in previous years, the range of issues we deal with continues to expand rapidly. So too does our responsibility to individuals across Ireland and the EU. The main drivers are the unrelenting pace in the growth of the internet and technological innovations such as artificial intelligence and the Internet of Things, as well as the continuing presence in Ireland of most of the world's leading technology and internet companies.

At EU level, we are active participants in the Article 29 Working Party – comprising the national data-protection authorities (DPAs) in Europe – working closely with EU colleagues to harmonise the application of data-protection rules throughout the EU and to prepare for the coming into force of the General Data Protection Regulation (GDPR) on 25 May 2018.

Replacing the existing 1995 EU Data Protection Directive with a modernised code, the GDPR significantly increases the accountability and compliance obligations on organisations, while also providing for additional and stronger enumerated rights for individuals. Allied to this, the proposed new ePrivacy Regulation will also vest responsibility in the DPC for overseeing a range of matters specifically relating to privacy and data protection in the electronic communications sector. This new legal framework will also form the basis for much greater cooperation between European data-protection authorities. In particular, the DPC's role under the GDPR will become a central one in Europe as a lead supervisory authority for the regulation of many multinational companies that are established in Ireland.



Mr. John O'Dwyer



Ms. Anna Morgan



Ms. Helen Dixon



Ms. Jennifer O'Sullivan



Mr. Dale Sunderland

DPC Senior Management Team

In 2016, as part of the enhanced resourcing of the Office and in preparation for the GDPR, the leadership capacity and capabilities of the organisation were significantly boosted with the addition of three deputy commissioners to the senior management team. Our new deputy commissioners have extensive private- and public-sector experience and have brought a wide range of skills to the organisation, in areas such as legal, technology, strategy and policy development, private- and public-sector management and communications. The extended senior management team, along with additional specialist staff at heads of unit/assistant commissioner level, is allowing us to strengthen the capacity and professionalism of the DPC as an effective and proactive data-protection authority. See Appendix 4 for the DPC organisation chart.

Reflecting our significantly increased funding allocation and the rapidly growing size of the organisation, strengthened governance arrangements were put in place in 2016 with the formal establishment of the DPC Senior Management Committee (SMC), comprising the Commissioner and Deputy Commissioners. The SMC is mandated with the proper management and governance of the organisation in line with the principles set out in the Code of Practice for the Governance of State Bodies. The Committee's terms of reference include the strategic leadership, management and oversight of the organisation, and the monitoring of performance of our management and staff against our strategic and business priorities and objectives.

Our senior management team:

- **Ms. Helen Dixon** (Data Protection Commissioner)
- **Mr. John O'Dwyer** (Deputy Commissioner – Investigations, Audit and Transfers)
- **Mr. Dale Sunderland** (Deputy Commissioner – Consultation, Corporate Affairs and Communications)
- **Ms. Anna Morgan** (Deputy Commissioner – Head of Legal)
- **Ms. Jennifer O'Sullivan** (Deputy Commissioner – Multinationals and Technology)

Funding



Funding and administration

Dedicated funding for the DPC is channelled through the vote of the Irish Department of Justice and Equality. The DPC collects revenue from the statutory registration function of the Office, and that revenue is remitted directly back to the exchequer. Government funding of the DPC has increased significantly in recent years from €1.7 million in 2013 to €7.5 million in 2017. The 2016 allocation was €4.7 million. The Account of the Income and Expenditure for 2016 is at Appendix 5.

Fulfilling our mandate as the independent supervisory body in Ireland charged with upholding the EU fundamental right to data protection is dependent on sufficient resources being provided by government. The DPC acknowledges the significant increase in funding in recent years and welcomes the government's continuing commitment to meeting the resourcing needs of the Office.

Additional funding in 2016 was prioritised towards the continuation of our recruitment drive, with an emphasis on strengthening the organisation's skills base in the areas of legal, technology, audit and investigations. The remaining posts targeted for recruitment in 2016 were filled in early 2017, bringing our staff numbers to 61. Recruitment in 2017 will further increase our team to almost 100 in size, located across our offices in Dublin and Portlarlinton.

While the DPC is an independent body, we ensure that oversight of our administration follows the requirements set out for all public-sector bodies. All expenditure must be accounted for to the exchequer, and our accounts are audited annually by the Comptroller and Auditor General. Our daily interaction with citizens, businesses and other key stakeholders provides additional oversight of the work we undertake. Statutory decisions of the Commissioner can be appealed to the courts.

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

Staff



The Data Protection Commissioner's main goals for

- 1. GDPR and ePrivacy Readiness:** Input to government to ensure that the underpinning legislation for the GDPR/ePrivacy Regulation provides the powers that the DPC needs to effectively perform its functions; provision of clear, high-quality and timely guidance to data controllers and processors; engagement with and contribution to the Article 29 Working Party towards preparation of harmonised guidance; implementation of a new website and case-management system; restructuring of the DPC to enable it to deliver on its new enforcement role; continuation of high-volume outreach to stakeholders through speaking at conferences etc.; and upskilling of staff to meet new regulatory demands.
- 2. Recruitment:** Targeted recruitment of an additional 30-plus staff with data analytics, legal, technical, policy, process and efficiency improvement, investigative, communications and management skills.
- 3. Standard Contractual Clauses (SCCs) CJEU Reference Application to High Court:** Direction and management of the SCC proceedings in the most efficient and effective manner possible to maximise the prospects of securing a reference to the CJEU on the validity of SCCs, in light of the directions of the CJEU in its October 2015 ruling in 'Schrems 1'.
- 4. Investigations, Audits and Strategic Consultation:** Maximise the impact for data subjects of DPC audits, investigations and strategic consultation by continuing a programme that targets high-risk areas of personal data processing. Track progress using the dashboard on the new case-management system to be developed in the next 12 months.
- 5. Digital Clearing House:** Engage with the European Data Protection Supervisor initiative to drive closer engagement between competition, consumer and data-protection regulators to ensure that European data subjects and consumers are benefitting fully from 'fairness' in terms of the online services to which they subscribe.

Review of 2016 in brief

We dealt with
15,335
Queries via email

16,744
Telephone calls

1,150
by post

1,479
complaints
investigated

We
received
2,224
Data Security
Breach
Notifications

100+
meetings were held
with multinational
companies

- ✓ We dealt with **15,335** queries by email, **16,744** calls by telephone and **1,150** queries by post.
- ✓ **1,479** complaints were investigated, with the largest single category of complaints continuing to be access requests (56%).
- ✓ We received 26 '**Right to be Forgotten**' complaints, with 6 upheld, 15 rejected and 5 currently still under investigation.
- ✓ While the majority of complaints continued to be amicably resolved, we issued a record number of formal decisions, with 59 in total compared to 52 in 2015. **1,438** complaints were concluded in 2016, up from 1,015 in 2015.
- ✓ **2,224** valid data-security breaches were recorded, a decrease from 2,317 notifications reported in 2015.
- ✓ 2016 was the first full year of operation of the **Special Investigations Unit**. The ongoing investigation into the private-investigator sector remained a central focus, leading to two successful prosecutions.
- ✓ In 2016, the Special Investigations Unit finalised preparations to open a new investigation in the hospitals sector in 2017 to examine the processing of patient sensitive personal data in areas of hospitals with patient and public access.
- ✓ We set up a new Multinationals and Technology team so that our regulatory activities for each multinational are coordinated and effective. We had extensive interactions with multinationals on a variety of matters, including proposed new policies, products and services. **Over 100 face-to-face meetings** were held with multinational companies.
- ✓ During 2016, the DPC had many meetings and contacts with Facebook Ireland on a variety of data-protection and ePrivacy matters. One outcome was Facebook Ireland updating its cookie-banner notification to include more precise information on its usage of cookies for commercial purposes.
- ✓ As part of its ongoing engagement with the DPC, LinkedIn updated the information available to its members and visitors to its site on its use of cookies.
- ✓ We engaged in thorough examination of the WhatsApp Terms of Service and Privacy Policy following Facebook Inc.'s acquisition of WhatsApp in 2014.
- ✓ We investigated a data breach reported to the DPC by Yahoo!EMEA and Yahoo!Inc. in September 2016, whereby approximately 500 million Yahoo! user accounts had been copied and stolen from the Yahoo!Inc. infrastructure in 2014.

1,170
Consultation
Queries

We
carried out
50+
audits and
inspections

9
prosecuted
for electronic
marketing
offences

Presented at
60+
speaking
events

- ✓ Consultation queries rose significantly in 2016, from 860 in 2015 to a total of **1,170**. Over 100 face-to-face meetings were held with public- and private-sector companies.
- ✓ We carried out **50 audits and inspections** including in-depth audits of State agencies (e.g. An Garda Síochána, Revenue Commissioners Defence Forces and GSOC).
- ✓ 2016 saw the establishment of a **centralised legal unit** within the DPC.
- ✓ Prosecutions were taken by the Commissioner in 2016 for a range of offences committed under the Data Protection Acts and the ePrivacy Regulation. Nine entities were prosecuted for electronic marketing offences.
- ✓ **We commenced High Court proceedings in May**, seeking a reference to the CJEU to examine the validity of standard contractual clauses as a means of transferring EU personal data to the US. The hearing earlier this year ran for 21 days and shone a very bright spotlight on the considerable complexities of the laws and roles of the various actors relevant to this case including the European Commission and the US Government.
- ✓ **Promoting and building awareness of data protection** continued to be a key priority and we were actively engaged in providing guidance and communicating our key messages, using a broad range of communications channels, techniques and platforms. These included conferences and speaking events; engagement with the media and social media; guidance; and information-awareness-raising campaigns.
- ✓ In 2016, we maintained an extensive outreach schedule and actively engaged with a broad base of stakeholders through speaking at seminars, conferences and to individual organisations on over **60** occasions during the year.
- ✓ In October 2016, we launched our Twitter account **@DPCireland** to disseminate regular and key messages on our work, the GDPR and other important data-protection information. In the five months since the launch our tweets generated over 390,000 impressions and we have grown our national and international Twitter following to over 1,250.
- ✓ In 2016, the Commissioner and/or Deputy Commissioners attended all plenary meetings of the Article 29 Working Party, which acts as an advisor to the European Commission on data-protection issues. We participated in some 50 meetings in Brussels.
- ✓ In 2016, a **Global Privacy Enforcement Network (GPEN)** Privacy Sweep was conducted by 25 data-protection regulators around the world, including Ireland.

Contacts, Queries and Complaints

The DPC receives a high number of contacts, queries and complaints each year. Our information/complaints email facility received 15,335 queries in 2016; our telephone helpdesk received 16,744 calls; and we also received 1,150 queries by post.

We aim to resolve all queries and complaints in as short a time frame as possible, to the satisfaction of the querist. In many cases, we will provide the querist with appropriate advice in order that they themselves may resolve their data-protection issue as expeditiously as possible.

As well as assisting members of the public in resolving any data-protection queries/complaints they may have, we monitor the nature of complaints received in order to build up a picture of the data-protection issues that are causing most concern to members of the public at a particular point in time so that the necessary and appropriate action can be taken. For example, in August 2016 we published guidance on location data after receiving a number of queries. Guidance had not previously been published on this topic.

In 2016, a total of 1,479 complaints were investigated.

As in previous years, the largest single category of complaints involved access requests (56%), which is an indicator of data controllers not being aware of or complying with their statutory obligations in this area. The current statutory period to respond to an access request is 40 days. The GDPR, which takes effect from 25 May 2018, lowers the period for complying with an access request to one month.

The number of complaints concerning electronic direct marketing continues to remain relatively static, with 118 received in 2016 compared to 104 in 2015. The DPC regularly pursues prosecutions in this area under the Privacy in Electronic Communications Regulations (SI 336 of 2011). Of the 118 complaints received, 55 related to email marketing, 45 related to SMS (text message) marketing and 18 related to telephone marketing.

In 2016, preparations were finalised for information campaigns on access rights and electronic direct marketing to raise awareness on the rights of individuals and the obligations of organisations. These campaigns launched in 2017.

Right to be Forgotten

The so-called 'Right to be Forgotten' (RTBF) or internet-search-result delisting category of complaints emerged from 2014 onwards following the ruling of the 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 ruling).

Since the ruling, internet users across Europe can, in certain circumstances, ask search engines to delist information about them. Where the search engine refuses, data subjects may bring the matter before their national data-protection authority. It is important to point out that the RTBF case concerns delisting specifically in cases of searches under the individual's name.

The DPC received 26 complaints in 2016 of which 6 were upheld, 15 were rejected and 5 are currently still under investigation. The criteria for delisting involves an analysis of whether the search results are inaccurate, irrelevant or out of date.

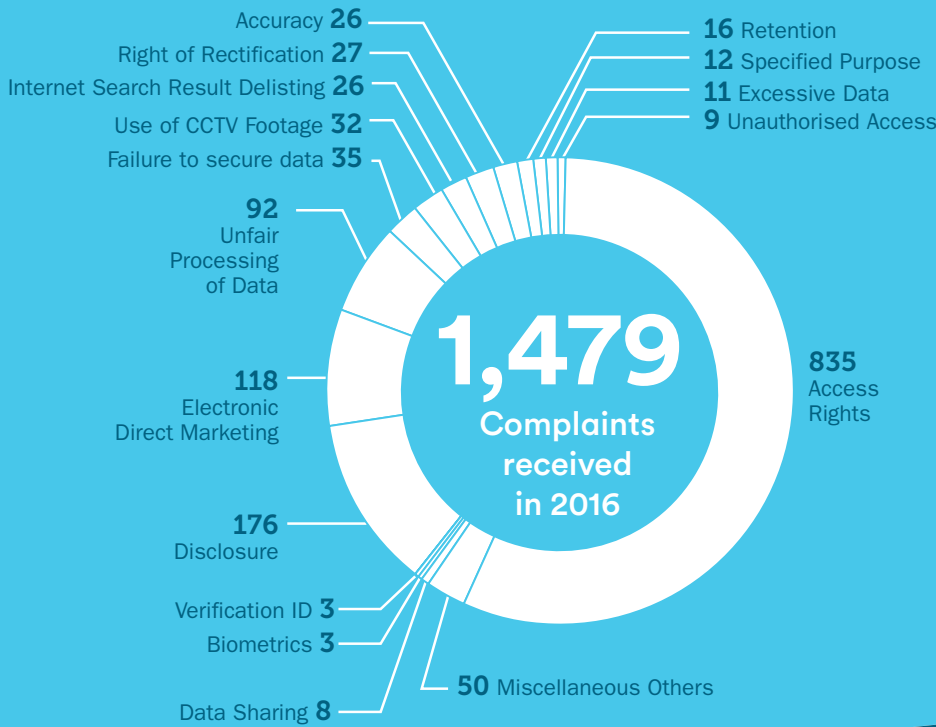
Of the complaints that were upheld, one related to the reporting of an individual's conviction for assault causing harm for which the individual was sentenced to six months' imprisonment suspended for three years. Given that seven years had passed from the date of the conviction, it qualified as a spent conviction under the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016. We considered that the story was no longer relevant on this basis, and the search engine removed the link in question.

Conclusion of complaints

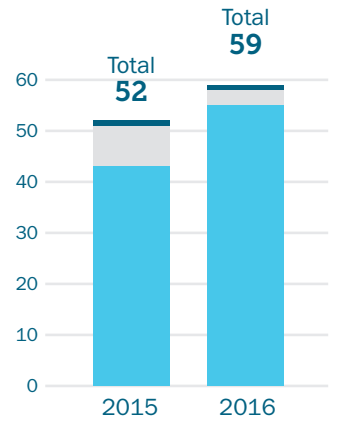
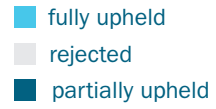
It is the statutory obligation of the DPC to strive to amicably resolve any complaints we receive from members of the public. Throughout 2016, the vast majority of complaints were successfully concluded amicably between the parties to the complaint without the necessity for issuing a formal decision under Section 10 of the Data Protection Acts. In 2016, the Commissioner issued a record number of formal decisions: 59 in total of which 55 fully upheld the complaint, 1 partially upheld the complaint and 3 rejected the subject of the complaint. The comparable figures for 2015 were 52 formal decisions of which 43 fully upheld the complaint, 1 partially upheld the complaint and 8 rejected the subject of the complaint. A total of 1,438 complaints were concluded in 2016. In 2015, a total of 1,015 investigations of complaints were concluded.

Case studies in relation to these complaints are at Appendix 2.

Breakdown of complaints by data protection issue



Formal decisions 2015 vs 2016



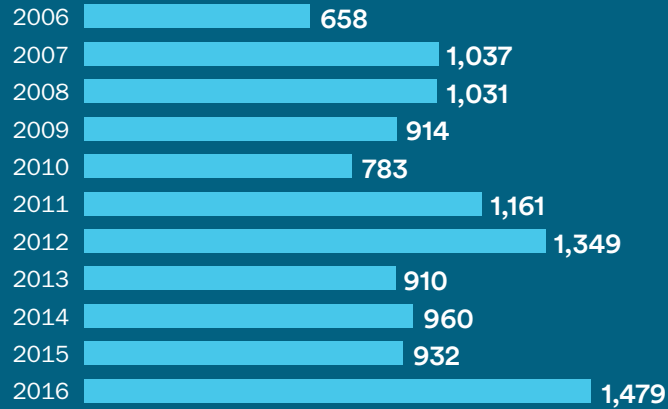
Overview of Complaints 2016

1,479
Complaints received

1,438
Complaints concluded

508
Complaints outstanding at end of year

Number of complaints received since 2006



Right to be forgotten



Special Investigations

2016 was the first full year of operation of the Special Investigations Unit.

2016 was the first full year of operation of the Special Investigations Unit. The unit was established primarily to carry out investigations on its own initiative, as distinct from complaints-based investigations.

Private Investigator Sector

The ongoing investigation into the private-investigator sector remained a central focus of the work of the Special Investigations Unit in 2016. Arising from investigations conducted by the unit, two prosecutions were successfully undertaken in 2016.

As these cases demonstrate, a significantly high level of breaches by some private investigators have been uncovered since the concerns in this area first came to light in 2013. In 2016, the investigation was extended across all sectors that use private-investigator services on a regular basis – such as banks, insurance companies, law firms and financial services companies. In the event that our investigation finds evidence of further offending behaviour by private investigators, the DPC will prosecute those offences.

Case Study 1

Prosecution of James Cowley Private Investigator

James Cowley was charged with 61 counts of breaches of the Data Protection Acts 1988 and 2003. All charges related to breaches of Section 22 of the Data Protection 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. The personal data was disclosed to entities in the insurance sector – the State Claims Agency, Zurich Plc and Allianz Plc.

On 13 June 2016, at Dublin Metropolitan District Court, James Cowley pleaded guilty to 13 sample charges. He was convicted on the first four charges and the court imposed a fine of €1,000 in respect of each of these four charges. The remaining nine charges were taken into consideration in the sentence imposed.

The investigation in this case uncovered access by the defendant to social-welfare records held on databases in the Department of Social Protection. To access these records, the defendant used a staff contact who was known to him. Mr Cowley then used the information he had obtained for the purposes of compiling private-investigator reports for his clients. These activities continued for a number of years up to September 2015, when our investigation team first made contact with him about its concerns in relation to his processing of personal data.

Another subject of concern that came to our attention in the private-investigator sector in 2016 was the use of vehicle-tracking devices by some private investigators. If an organisation hires a private investigator to conduct tracing or surveillance on an individual and that private investigator attaches a vehicle-tracking device on the individual's car, for example, during the course of their operations, clearly the purpose of the device is to track the individual's movements and location based on the movement and location of their car. It is this monitoring of the individual's location data that engages the protections of the Data Protection Acts 1988 and 2003.

Within the framework of the data-protection legislation, private investigators are generally deemed to be data processors operating for the organisation that has hired them. Data controllers are obliged to set down instructions for data processors relating to data-processing tasks and ensure that the data processor works to those instructions and complies with its data-protection obligations in doing so. If a private investigator was to stray outside of the instructions of the hiring data controller by attaching vehicle-tracking devices to monitor individuals, then this would likely pose difficulties for the data controller in relation to compliance with Section 2(C)3 of the Data Protection Acts.

During 2016, our Special Investigations Unit contacted almost 400 companies or organisations that we know to be current users, or potential future users, of private-investigator services to alert them to this issue. We recommended that they write to all private investigators on their panels to, among other things, put them on notice that the use of vehicle-tracking devices should not occur without the consent of the vehicle owner concerned.

While the Special Investigations Unit's main focus is on investigations of its own initiative, as distinct from complaints-based investigations, the unit handled four investigations in 2016 that arose from complaints received from the general public concerning the activities of private investigators.

Surgical Symphysiotomy Payment Scheme

On foot of a complaint received in March 2016, the Special Investigations Unit initiated an investigation into the Surgical Symphysiotomy Payment Scheme and its plan to shred certain documents which were submitted to it by applicants as part of their claims for redress under the Scheme. As part of the investigation, a physical inspection was carried out at the offices of the Surgical Symphysiotomy Payment Scheme. Having examined all the files that were categorised for shredding by the scheme, the investigators were satisfied that the scheme had obtained appropriate and valid consent of applicants who had opted to have their documents shredded. The investigation concluded that no data breach had occurred to date in relation to the scheme's proposal to shred copies of applicants' documents and that no data breach will occur when the scheme proceeds to shred the applicants' application forms and copies of supporting documents in respect of deceased applicants and in respect of applicants who have opted to have their documents shredded.

The Hospitals Sector

In 2016, the Special Investigations Unit finalised preparations to open a new investigation in the hospitals sector in 2017. This investigation will examine the processing of patient sensitive personal data in areas of hospitals in Ireland with patient and public access; based on the findings of that examination it may make recommendations for improvements. It will involve physical inspections at hospitals across the State, spanning 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. This investigation will focus on the circulation and journey of patient files in order to identify whether there are any shortcomings in terms of meeting the requirements of the Data Protection 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.

Data Breach Notifications

During 2016, we received a total of 2,301 data breach notifications – of which 77 cases were classified as non-breaches under the provisions of the DPC Personal Data Security Breach Code of Practice.

A total of 2,224 valid data-security breaches were recorded during the period 1 January–31 December 2016. This represents a decrease from 2,317 notifications reported in 2015.

Telecommunications and internet service providers have a legal obligation under SI 336 of 2011 to notify the DPC of a data-security breach no later than 24 hours after initial discovery of the breach. If the provider is unable to provide full details on the breach at this time, further details should be provided within three days of the initial notification. Any telecommunications company that fails to notify the DPC of a data-security breach may be liable on summary conviction to a class-A fine or, on indictment, to a fine not exceeding €250,000.

In 2016, a total of 142 valid data breach notifications were received from the telecommunications sector. This accounted for just over 6.3% of total cases reported for the year, representing an increase from the 104 notifications reported in 2015.

All other data-security breaches reported to us are done so under a voluntary Personal Data Security Breach Code of Practice, which was introduced in July 2011. This Code of Practice is not legally binding and does not apply to the telecommunications sector. However, the General Data Protection Regulation, effective from May 2018, will make the reporting of data breaches to the DPC mandatory.

As in 2015, the highest category of data breaches reported under this Code of Practice involved unauthorised disclosures such as postal and electronic disclosures – the majority of which occurred in the financial sector – and such breaches accounted for just over 43.5% of total data breach notifications received in 2016.

Typical examples of data breaches reported include:

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

2016 also saw a rise in the number of network-security compromises reported to the DPC, with the number of notifications almost doubling from 12 cases reported in 2015 to 23 in 2016. Such cases typically include ransomware and malware attacks.

There was also an increase in website-security breaches reported, up from 12 in 2015 to 16 in 2016. These types of cases usually involve online retailer sites that hold customer credit-card information; the attacker is primarily focused on scraping credit-card details from the site for fraudulent purposes.

IT-related data breaches are dealt with by the Multinationals and Technology team, who review the actions taken by data controllers in response to a such a breach and, where appropriate, advise organisations on further measures to strengthen system security to ensure non-recurrence of such IT-related breaches.

Data Breach Notifications - 2016

2,301

data breach notifications

3.3% (77)

cases were classified as non breaches - under the provisions of the Personal Data Security Breach Code of Practice.

2,224

valid data security breaches recorded by the Office

(01 Jan – 31 Dec 2016)

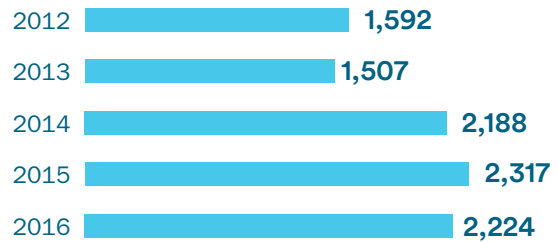
↓ 4.18% (93)

decrease on the numbers reported in 2015.

Breach Notifications by Category and Type of Data Controller - 2016

| Category | All Sectors | Public Sector | Private Sector |
|--------------------------------------|--------------|---------------|----------------|
| Theft of IT Equipment | 14 | 9 | 5 |
| Website Security | 103 | 18 | 85 |
| Unauthorised Disclosure – Postal | 570 | 100 | 470 |
| Unauthorised Disclosure – Electronic | 376 | 176 | 200 |
| Unauthorised Disclosure – Other | 1,117 | 244 | 873 |
| Security related issues | 44 | 18 | 26 |
| Non Breach | 77 | 20 | 57 |
| Total | 2,301 | 585 | 1,716 |

Comparison of Breach Notifications 2012 - 2016



Comparison of Organisations making Breach Notifications 2012 - 2016



Case Study 2

Disclosure of Personal Data to a Third-party in Response to a Subject Access Request

An ex-employee of Stobart Air made a complaint in August 2015 to us regarding the unlawful disclosure of their redundancy details to another member of staff following an access request made by that person to the company. The complainant also informed us that they had equally received third-party personal information in response to a subject access request that they themselves had made to the company in May 2015.

Stobart Air, on commencement of our investigation, confirmed to us that a breach of the complainant's data had occurred in November 2014. It stated that it had not initially notified the complainant of the breach when it had first learned of it as it had been unaware of the data-protection guidelines that advise the reporting of disclosures to the data subjects involved where the disclosure involves a high risk to the individual's rights and requesting the third party in receipt of the information to destroy or return the data involved.

The complainant in this case declined an offer of amicable resolution and requested a formal decision from the Commissioner. In her decision, the Commissioner found that Stobart Air, in including the complainant's personal data in a letter to ex-employees, had carried out unauthorised processing and disclosure of the complainant's personal data. This had contravened Section 2A(1) of the Data Protection Acts 1988 and 2003, by processing the complainant's personal information without the complainant's consent or another legal basis under the Data Protection Acts 1988 and 2003.

Stobart Air itself identified that it had inadequate training and safeguards around data protection in place, which it has since sought to rectify.

In a separate complaint received by the DPC in September 2015, we were notified that Stobart Air had disclosed financial data of a third party to the complainant in response to a subject access request. We proceeded to remind Stobart Air of its obligations as a data controller and Stobart Air identified a number of individuals who had been affected by these issues. Stobart Air subsequently notified all affected third parties of the breach of their personal data. However, in trying to comply – by notifying the affected individuals – Stobart Air disclosed the complainant's data, divulging the fact that the complainant was the recipient of this data in a letter notifying the individuals whose data had been originally disclosed.

Stobart Air had no legal basis to disclose the complainant's personal data to the third parties involved nor did it have consent of the individual affected. The disclosure of the complainant's identity to the individuals affected by the original breach was unnecessary in the circumstances and in contravention of Section 2A(1) of the Data Protection Acts 1988 and 2003.

Multinationals & Technology

Our supervision of multinationals with bases in Ireland was ongoing during 2016. This supervision of multinationals is now being delivered by the new Multinationals and Technology team at the DPC, ensuring that our regulatory activities for each multinational are coordinated and that we are well-placed for the introduction of the GDPR and its one-stop-shop provisions in May 2018.

The team now leads on all consultations, investigations and audits that relate to cross-border processing by multinationals. As our regulatory work with multinationals is most often with companies that are technology-focused, most of the work of the section has a technology emphasis and is delivered by technology specialists on the team. The section also supports the work being led by other units of the DPC by providing inputs on technology and data-security aspects, as required.

During 2016, we recruited specialist resources for this team, and will continue to build our capability and capacity during 2017.

Once the GDPR comes into force on 25 May 2018, the DPC will be the lead data-protection authority for the regulation of multinationals that have their 'main establishment' in Ireland under the one-stop-shop model. This model also requires us to cooperate with other data-protection authorities on a regular basis on cases related to cross-border data processing. The Multinationals and Technology team will become the coordinating hub for this work, so that we can discharge our obligations most effectively and efficiently.

During 2016, we had numerous interactions with several multinationals on a variety of matters, including proposed new policies, products and services. Discussions with multinationals on their preparations for the introduction of GDPR also commenced during 2016, and we expect this type of engagement to scale up during 2017.

The new Multinationals and Technology team now leads on all consultations, investigations and audits that relate to cross border processing by multinationals.

Examples of our engagement with multinational companies during 2016, which included more than 100 face-to-face meetings, are as follows:

- Through consultation between Facebook Ireland and the DPC, Facebook Ireland updated its cookie-banner notification to include more precise information on its usage of cookies for commercial purposes.
- Similarly, LinkedIn updated the information available to its members and visitors to its site on its use of cookies, as part of its ongoing engagement with the DPC.
- Consultation with Apple on the review of its new education service.
- Engagement with Google on changes to its terms and on its approach to online behavioural advertising.
- Several meetings with organisations exploring the possibility of establishing in Ireland as either a data controller or processor.
- Examination of the WhatsApp Terms of Service and Privacy Policy – see below.
- Investigation of Yahoo! Breach – see below.

High-profile cross-border cases

In the latter part of 2016, two separate matters arose relating to technology multinationals, with each being the subject of significant national and international media coverage. The Multinationals and Technology section has applied significant resources in the rigorous assessment and resolution of both of these matters.

The first was WhatsApp's update to its Terms of Service and Privacy Policy in August 2016, including references to the sharing and matching of WhatsApp user data with Facebook user data. This followed Facebook Inc.'s acquisition of WhatsApp in 2014. As the data controller for Facebook users who live outside the US and Canada, Facebook Ireland is a party to this sharing and matching of user data. The DPC has been engaged directly with both Facebook Ireland and WhatsApp over the past months to address the concerns that arose on how WhatsApp users' consent was obtained for this data sharing and on the purposes and means of processing for this data sharing.

The DPC has emphasised the importance of Privacy by Design through the full product lifecycle in our engagement with Facebook and other technology multinationals.

The second was the data breach reported to the DPC by Yahoo!EMEA and Yahoo!Inc. in September 2016, whereby approximately 500 million Yahoo! user accounts had been copied and stolen from the Yahoo!Inc. infrastructure in 2014. Yahoo!EMEA is the data controller for the subset of these stolen user accounts associated with EU/EEA citizens, and Yahoo!Inc. acts as the data processor. During the course of the DPC's investigation into this specific data breach, Yahoo!EMEA has reported further separate data breaches to the DPC related to the Yahoo!Inc. infrastructure, which are also in the public domain, and which we continue to assess.

The DPC expects both of these matters to be concluded during 2017.

Engagement with Facebook Ireland

During 2016, the DPC had many meetings and contacts with Facebook Ireland on a variety of data-protection and ePrivacy matters, including on matters carried over from 2015. We reviewed terms, policies and product updates, and provided best-practice recommendations and guidance, with our feedback being contextualised to the introduction of the GDPR in May 2018. Our engagement covered many aspects of Facebook's services, from apps and website functionality, to the scope and possible improvements to existing data-protection tools available to users, to the use of new technologies and their impacts on individuals' rights. This two-way interaction between the DPC and Facebook allows us to understand Facebook's service more fully and to seek compliance-based solutions to issues.

Updated Cookie Banner and Policy

How to provide transparency and clear notification to users about Facebook's use of cookies was a key theme during 2016. This issue arises for both registered users and for visitors to the Facebook service. Under ePrivacy, data controllers are required to gain consent for cookie storage and to provide prominently displayed information about the purposes of processing.

In 2016, after engagement with the DPC and other stakeholders, Facebook Ireland updated its cookie-banner notification to include more precise information around its usage of cookies for commercial purposes. Facebook emphasised to users that it required a clearly signalled action to indicate that the users were consenting to these purposes.

Facebook has also updated its cookie statement to include more information related to cookie usage beyond the facebook.com site, and expanded the information in its tabulated list of cookies.

These changes bring benefits to both Facebook users and visitors, by increasing their awareness and control of the use of their equipment for targeted advertising purposes. The changes apply both on and off the Facebook website, and seek to improve the quality of informed consent that users and visitors provide.

Software Engineering Practices

Privacy issues caused by the functionality of websites and apps can originate during the software design and development stages, potentially due to lack of awareness and training, or to quality assurance and governance practices, or through maintenance and regression-testing approaches. This can be an issue for many internet service providers – not just Facebook – but the scale of Facebook's user base means that any issues can be significant.

In 2016, we received notification from an individual that a profile photo they had previously deleted on Facebook was still available sometime later. We determined that the problem was related to a historic software bug on Facebook, which we had previously confirmed through our own testing as being resolved by Facebook. Our analysis that the bug had potentially re-emerged was confirmed by Facebook. Facebook had been faced with a need to expand the capacity of its image-handling systems, with the continual growth of photo usage on the platform. This had involved the migration from the legacy image-handling systems to a new system, which resulted in some photos persisting on the system incorrectly. We are satisfied that this particular issue is now completely resolved.

The identification of this issue highlighted to Facebook that continued vigilance and quality controls in its Privacy by Design practices are critical, from the initial product-development stage right through to the ongoing maintenance and enhancement of existing systems. The DPC has emphasised the importance of Privacy by Design through the full product lifecycle in our engagement with Facebook and other technology multinationals. This emphasis will be further underlined with the coming into force of the GDPR in May 2018, in that data controllers and processors have accountability to fulfil their data-protection obligations.

Engagement with LinkedIn Ireland

The DPC's supervision of LinkedIn Ireland has been very productive in recent years at a time of ongoing enhancement and expansion of LinkedIn's services. The DPC had several engagements with the representatives of LinkedIn Ireland during 2016. This engagement resulted in transparent updates to LinkedIn members on its account settings and in the introduction of a cookie-banner notification to meet ePrivacy requirements. We will continue to be actively engaged with LinkedIn Ireland in 2017 on any changes to its services and operations that may impact the data-protection rights of individuals, and also as LinkedIn Ireland prepares for the introduction of the GDPR and any privacy changes that may arise from its acquisition by Microsoft.

Updated Account Settings

In early 2016, LinkedIn Ireland notified the DPC that it would be continuing its work on updating personal data controls and settings that are available to its members. These allow LinkedIn users to control various aspects of how their personal data is used on the service, from email-notification frequency to the extent to which user-profile information is visible to others on the service. The updates included layout and formatting changes to improve access to the settings, and some default setting changes that aimed to increase the protection of personal data provided to LinkedIn.

This means that settings should be easier to find and use, that contact-information visibility is now even more restricted by default, and that it is possible to control connection suggestions more effectively. In addition, LinkedIn has strengthened some elements of the settings to require a secondary security step in cases where the impact of making changes might be high. This now occurs, for instance, when members choose to change their primary email setting, to block users, or to make changes to enhanced login checks.

We welcome these significant changes as a step forward in LinkedIn's compliance with the data-protection requirements, and in the support and consideration it is offering members in terms of transparency and control. This work will need to continue in preparation for the introduction of the GDPR and the anticipated new ePrivacy Regulation.

Cookie Notification

Further to our audit in 2013, our follow-up implementation review in 2015 and our continued engagement in 2016, LinkedIn Ireland again updated the information available to its members and visitors on its use of cookies. LinkedIn has also added a prominent notification banner to the site, alerting members and visitors to cookies and providing a link to the updated information available in its cookie statement.

This statement now includes information on the online behavioural advertising purposes of its cookies, a detailed table of cookies in use, and direct links to the relevant opt-outs from both its own advertising programme and from third-party cookie usage on its site.

We welcome the increased transparency for LinkedIn members and visitors alike as a further improvement in the quality of consent under ePrivacy Regulation (SI 336/2011), and the options available to non-members regarding LinkedIn cookies on other sites. We are continuing to review the information available to members and the notification made to them concerning the use and purposes of cookies, especially in light of the consent requirements in the upcoming GDPR and the possible changes that may arise under the new ePrivacy Regulation.

Common Technology Issues

During 2016, the Multinationals and Technology section handled a wide variety of technology-related complaints, completed detailed assessments of varying types of breaches, and proactively audited and inspected diverse organisation types. Within this wide variety, there were three common data-protection issues that we identified most often.

First, many data controllers are not fully aware of their obligations, or do not discharge their obligations fully, in their engagement of data processors, as required by the Data Protection Acts. This hands-off approach to governance of data processors can have a significant impact on the strength of the security measures that are in place to protect personal data, and consequently on the vulnerability of the personal data. Data controllers must obtain sufficient guarantees that the processor's security measures are appropriate and up to date, and that the processor's staff are fully aware of these measures. A data-processing

agreement or contract that sets out the obligations of the processor must be in place and, very importantly, there should be regular and meaningful assessment by the controller of the processor's compliance with those obligations.

A second common issue relates to the suite of security measures that organisations have in place. These measures need to be multi-faceted so that the different types of risk to personal data are mitigated as far as possible. We identified many organisations that were overly reliant on one type of security measure, while not addressing other types of vulnerability. Security measures should cover technical risks through the deployment of up-to-date security infrastructure, organisational risks through the enforcement of rigorous policies, procedures and inventories, and human-error risks through training and awareness.

Finally, many attacks that resulted in personal-data loss depended on human misjudgement or error for their success. Attack types such as ransomware may be avoided by an organisational standard of 'think before you click'. In seeking to quickly solve one operational issue, infrastructure engineers should always ensure that a new vulnerability has not unwittingly been introduced, for example, via open ports.

We will continue to issue practical guidance notes and advice during 2017 on these common issues and other emerging technology trends, and these will also drive our planning of multinational audits for 2017

Case Study 3

Data Breach at a Retail and Online Service Provider

In July 2016, we received a breach report from an organisation providing retail and online services.

The organisation was victim of a 'brute force' attack, whereby over a two-week period the attackers tried various username/password combinations, with some combinations successfully being used to gain access to user accounts. When these accounts were accessed, the attackers attempted to withdraw user balances. These withdrawals were enabled by the attacker having the ability to add new payment methods. It was also possible for the attacker to access the personal data associated with the account.

On assessing the breach, we identified that the organisation had deficiencies in the measures it had taken to secure users' personal data, including:

- insufficient measures on password policy and user authentication;
- insufficient control measures to validate changes to a user's account; and
- insufficient control measures on the retention of dormant user accounts.

We considered that the organisation contravened Section 2(1)(d) of the Data Protection Acts 1988 and 2003 by failing to take appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure or destruction of, its users' personal data.

Recommendations were issued to the organisation that it take steps to mitigate the deficiencies identified or face enforcement action. The organisation subsequently informed us that it had taken the following steps based on our recommendations:

- implementation of passwords that require more than one factor; and
- implementation of a comprehensive data-retention policy.

This case highlights the need for organisations to ensure that they have appropriate technical organisational and security measures in place to prevent loss of data through 'brute force' or reuse of password attacks. In this scenario, the use of appropriate access and authentication controls, such as multifactor authentication, network rate limiting and logon alerts, could have mitigated the risks. Further, poor retention policies provide an 'attack vector' for hackers, such as that used as a means of entry in this breach.

Consultation

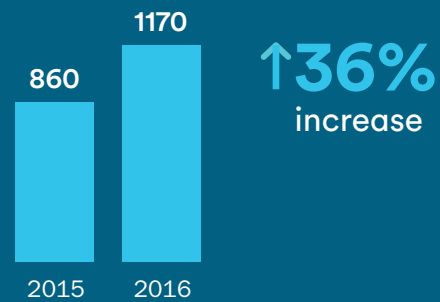
The consultation function plays a pivotal role in advancing a better understanding and awareness of data-protection obligations. Through active and meaningful engagement with both public- and private-sector organisations we are delivering on our remit to ensure that data controllers are responsible and compliant with data-protection legislation and that protection of fundamental right is at the forefront of any project involving the processing of personal data. We believe that the biggest gains in terms of widespread protection of the public from poor personal-data-handling practices come from the consultation work we do with all types of organisations. Driving compliance, and ensuring that organisations consider the importance of the backdrop of the Charter of Fundamental Rights of the European Union, means fewer systemic issues arise.

Consultation queries rose significantly from 860 in 2015 to a total of 1,170 in 2016, representing a 36% increase. The breakdown of consultation queries received was evenly divided between the public and private sectors. It appears that this increase can be attributed to a number of factors including: preparation by data controllers for the GDPR; and a growing public awareness of the importance of data-protection issues and rights.

It is expected that this growth trend will continue for 2017 given the increasing level of awareness of individuals of their data-protection rights as well as a growing acceptance by organisations that compliance with data protection is a key and imperative component to the successful delivery of projects/ventures that involve the processing of personal data. The implications of the new General Data Protection Regulation are also coming into sharp focus and we will be publishing guidance throughout 2017 to assist organisations in preparing for its introduction on 25 May 2018.

In 2016, the consultation section proactively engaged with a wide range of stakeholders, providing the appropriate direction and guidance to allow data controllers to confidently make decisions about projects/proposals that involved a personal-data element. Over 100 face-to-face meetings were conducted during the year (this figure does not include meetings with multinational companies. See section on Multinationals and Technology for further details).

Consultation Queries



100+ face-to-face consultation meetings conducted

Some of the organisations/groups and projects (exploratory or otherwise) that we engaged with during 2016 included the following:

Public Sector:

- Department of Social Protection regarding data sharing
- National Data Infrastructure/Ecosystem
- Public Services Card
- Central Statistics Office
- Local-authority councillors regarding access to housing lists
- Various local authorities – litter dumping, data-sharing arrangements
- Public-sector bodies regarding the use of body-worn cameras
- Road Safety Authority
- National Board for Safeguarding Children in the Catholic Church

2016 saw an emerging trend towards name and shame style campaigns by public sector organisations.

Health Sector:

- Individual Health Identifier
- National Medical Laboratory Information System (MedLIS)
- The Children's Hospital
- Diabetes Type II Database
- Doctors and Irish Medical Council
- Genetic Data and Health Research
- National Medical Oncology Clinical Information System
- Electronic Patient Records (EPR), neonatal and maternal
- Mount Carmel Hospital (in liquidation)

Comprehensive observations on draft legislation were also made to various government Departments during 2016. These included:

- Draft Adoption (Information and Tracing) Bill 2016
- Draft Heads of Bill, Amalgamation of the Financial Services Ombudsman and the Pensions Ombudsman Offices
- General Scheme of National Archives (Amendment) Bill 2016
- Health Information and Patient Safety Bill 2015
- Student Support Act 2011 (additional bodies under Schedule 2)

Private/Financial Sector (excluding multinationals sector):

- Central Bank of Ireland/Credit Reporting Register
- Health Insurers (claims)
- Banking and Payments Federation Ireland
- Credit Unions
- IBEC (Retail sector & Telecommunications and Internet Federation)
- Financial Services Ombudsman Bureau
- Dublin Airport Authority
- Irish Mortgage Holders Organisation

Name-and-shame Proposals

2016 saw an emerging trend towards name and shame style campaigns by public sector organisations. Public sector bodies who seek to implement name and shame type initiatives need to be sure the evidence is clear, that the naming and shaming produces the desired outcomes and that those outcomes cannot be achieved without interfering with privacy rights. Where implemented the rights of individuals must not be overly prejudiced. Additionally, where name and shame initiatives proceed, the necessary safeguards must be put in place to ensure the data of innocent third parties is not inadvertently processed, or the wrong individual named or lists left published in perpetuity.

Inadequate Assessment

In 2016, we observed from all sectors an inertia at project-planning stage in carrying out data-protection assessments of data-processing proposals. It is incumbent upon all data controllers to take a detailed evidence-based approach. This must include a proper assessment that interrogates the various interests and data-protection issues arising and appropriately substantiates why data-protection rights of an individual must cede – in a proportionate way – to their legitimate interests.

A Data Protection Impact Assessment is a best-practice approach. It is a process of systemically considering the potential impact that a project/initiative would have on the privacy of individuals. It will allow for the identification of potential privacy issues but also provide guidance on how to appropriately address such issues in advance of processing and during the lifecycle of a project/initiative itself. The findings are based on discussions with relevant parties/stakeholders. Ultimately, such an assessment may prove invaluable in determining the viability of a project/initiative in the future.

Following the anticipated publication of the Article 29 Working Party's guidance on GDPR Data Protection Impact Assessments (DPIAs) in 2017, we will be publishing further guidance material on how to prepare a Data Protection Impact Assessment. Under the GDPR, from May 2018, DPIAs will be mandatory for certain types of data processing.

Privacy Audits

In 2016, 50 audits and inspections were carried out (the list of organisations audited is at Appendix 1). The aim of all our audits and inspections is to check for compliance with the Data Protection Acts and to assist the data controller or data processor in ensuring that their data-protection systems are as effective and comprehensive as possible. Audits are sometimes supplementary to investigations carried out by the DPC in response to specific complaints. We identify priorities and targets for audit 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 contacts, queries and complaints that we receive.

The DPC's technical-audit capability was significantly strengthened during 2016 by the establishment of the Multinationals and Technology section. Specialist resources were recruited to provide technical-audit and data-security expertise to privacy audits, and to build capacity for the ongoing audit programme focused on technology multinationals.

Our annual audit programme is tailored to focus on a number of carefully selected sectors. In 2016, we conducted in-depth audits of State agencies (An Garda Síochána, Revenue Commissioners, Defence Forces and GSOC) prescribed under the Communications (Retention of Data) Act 2011, which make requests for data to communication service providers. Also selected for close examination was PeoplePoint on foot of the large number of data breaches being reported to the Office. In addition, audits were conducted of Cavan General Hospital, the Residential Institutions Redress Board and the Europol National Unit in Garda HQ, Phoenix Park.

Audits of private-sector entities included Allianz, Vhi, Laya Healthcare, Meteor and Eir. A number of retail outlets written to by the DPC as part of a data-protection sweep on credit cards were selected for audit in order to learn more about the retention of credit-card details by retailers. We will continue to examine this area in 2017.

An Garda Síochána, Defence Forces, Revenue Commissioners and Garda Síochána Ombudsman Commission – Communications (Retention of Data) Act 2011

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 publicly 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 (GSOC) and the Competition and Consumer Protection Commission (CCPC).

The DPC's oversight role is to ensure that all disclosure requests made are in compliance with the Data Protection Acts 1988 and 2003 and the Communications (Retention of Data) Act 2011.

Given the powers invested under Section 10(1A) of the Data Protection Acts, audits of the procedures and systems for processing disclosure requests within all prescribed State agencies were conducted, with over several hundred disclosure requests to CSPs examined

General Findings and Recommendations

Overall, we concluded that strict assessment criteria were deployed by the centralised liaison units in each State agency for every request sent to a CSP. Of particular note was the attention given by these units when working with investigation units on the ground to ensure that the scope of disclosure requests are narrowed down and refined to the minimum at all times. The audit team found that the principles of proportionality, necessity and relevance were applied in all disclosure requests examined and all requests were reviewed signed and approved at the required level on a case-by-case basis.

The DPC team encountered the practice of making applications for IP-related data under Section 8 of the Data Protection Acts because providers of non-publicly available electronic communications services do not fall

within the scope of the 2011 Act. Section 8(b) of the Data Protection Acts allows for voluntary disclosure by a data controller/processor subject to consideration on a case-by-case basis as to whether not releasing the data would be likely to prejudice (that is, significantly harm) any attempt by organisations that have crime-prevention or law-enforcement functions to prevent or solve the commission of a crime or an offence.

The team concluded that there were no data-protection issues of concern arising as a result of the audits and thus the recommendations issued were of a best-practice nature and confined to procedural issues.

- It was recommended that consideration is given by An Garda Síochána, the Defence Forces, CPCC and GSOC to the publication of a manual similar to that published by the Revenue Commissioners outlining the policies and procedures by prescribed agencies used to make disclosure requests.
- Disclosure requests made to CSPs in relation to subscriber requests should not refer to both the Communications (Retention of Data) Act 2011 and Section 8 of the Data Protection Acts. The specific legislation under which the disclosure request is being made should be cited in each disclosure request.
- Other recommendations focused on internal audit arrangements, retention policies, procedural documentation, access logs and the cessation of the use of registered post as a channel for submitting disclosure requests to CSPs.

An Garda Síochána

The audit team found that the majority of the disclosure requests reviewed related to the investigation of serious offences. Other grounds on which a disclosure request can be made are for the purposes of safeguarding the security of the State and the saving of human life. In terms of the breakdown of the data sought, these encompass three different types of request: call-trace requests; subscriber-data requests; and IP requests. Over the three years reviewed, the team determined that almost two thirds of the requests by AGS were for subscriber data. We also encountered a significant number of requests relating to the prevention of the loss of human life, some of which entailed ‘pinging’ – a type of call trace used in missing-persons cases.

The team noted that requests to CSPs made by AGS relating to Internet Protocol (IP) data constituted only

3% of the total number of disclosure requests between 2013 and 2015.

Revenue Commissioners

Over the three years reviewed, the team observed that requests made by the Revenue Commissioners between 2013 and 2015 sought subscriber data in all cases with one exception. Call-trace data was sought in almost 60% of those same requests. In a very small number of cases, the requests to CSPs made by the Revenue Commissioners between 2013 and 2015 related to Internet Protocol (IP) data.

Defence Forces

As per Section 6(3) of the Communications (Retention of Data) Act 2011, all requests reviewed were confined to the ‘safeguarding of the security of the State’. The team determined that the majority of the requests made by the Defence Forces between 2013 and 2015 concerned mobile communications data.

Garda Síochána Ombudsman Commission

Over the three years reviewed, the team determined that almost 74% of the requests made by GSOC between 2013 and 2015 were for call-trace data.

Competition and Consumer Protection Commission

The Competition and Consumer Protection Commission informed the Office that it had not yet invoked the powers afforded to it under Section 6(3A) and therefore no disclosure requests were made to CSPs between 2013 and 2015.

We commenced a series of audits of disclosure requests processed by CSPs, beginning with Eir and Meteor in Q4 2016, and will continue with this programme of audits in 2017.

PeoplePoint

PeoplePoint provide an HR and pensions shared service for public-service bodies, managing the data of over 35,000 civil servants. In light of the sheer volume of personal data processed via the PeoplePoint shared service centre, an audit of PeoplePoint was conducted in May 2016. The focus of the audit centred on data breaches due to the high number of breaches notified to the DPC by PeoplePoint in 2015 and 2016. In total, 163 breaches were notified by the Data Breach Unit in comparison to 155 breaches reported in 2015.

The inspection team concluded that the vast majority of data breaches within the organisation occurred as a result of human administrative errors. Overall, the team considered that there was not an acceptable level of awareness of data-protection principles in evidence generally within PeoplePoint in light of the number of breaches being reported by PeoplePoint to the DPC. We accept, however, that the vast majority of data breaches occurred through the issuing of data in error belonging to one public-sector body to an HR official (or officials) in another public-service body, with all HR officials concerned governed by the Official Secrets Act.

A key conclusion of our findings is that while high-level policies on data governance have been put in place, these have not filtered down sufficiently to an operational level. We consider it imperative that demonstrable steps are taken by PeoplePoint to ensure that the role of PeoplePoint is correctly understood by staff in their administration of all schemes. Hence, the audit report highlighted a need for more intense training for staff generally on data-protection matters as well as a focus on the role of data protection in relation to HR issues and specifically in relation to previous breaches. It is the intention of the Office to monitor closely the number of breaches reported in 2017 and to follow up accordingly.

Laya Healthcare and Vhi

In 2016, we received information from a GP practice on a request they had received from a health insurer seeking certain medical records of a patient, citing Section 4 (access requests) of the Data Protection Acts 1988 and 2003 and enclosing a cheque for €6.35.

We conducted audits of Laya and Vhi and advised both organisations that (even with the signed consent of the data subject), making a Section 4 access request to a medical practitioner in connection with a health-insurance claim may not be in line with the provisions of the Data Protection Acts. In general, Section 4 access requests should only be made by individuals seeking copies of their personal data for their own needs and not the requirements of a third party in a commercial context or otherwise. The reason for this is that an individual must be able to control which of their personal data they hand over to the insurer rather than risking their full medical file being unnecessarily disclosed.

We will continue with this programme of audits in 2017.

A key conclusion of our findings is that while high-level policies on data governance have been put in place, these have not filtered down sufficiently to an operational level.

Audit Findings

Themes identified in the 2016 audits include the following:

1. Employers seeking PPSN

An employer should only seek the PPSN of a prospective employee if they are successful in the recruitment process and are actually taking up employment with the organisation. While an employer requires the PPSN of each employee for Revenue purposes, there is no basis for an employer to capture a candidate's PPSN at the application stage.

2. Data Retention

Section 2(1)(c) of the Data Protection Acts 1988 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. In determining appropriate retention periods for personal information, data controllers must have due regard for any statutory obligations. If the purpose for which the information was obtained has ceased and the personal information is no longer required, the data must be deleted or disposed of in a secure manner.

3. Security of Sensitive Data

When an organisation is processing sensitive personal data, for example medical data, appropriate security standards must be in place at all times. Organisations must assure themselves that the procedures governing the processing of sensitive personal data are carried out in compliance with the Data Protection Acts and that the data is securely held. This may include a system of internal oversight such as a security review.

4. CCTV Policy and Signage

If an organisation is considering the use of CCTV, one of the key requirements that must be satisfied is the transparency of the system. Section 2D of the Acts requires that certain essential information is supplied to a data subject before any personal data are recorded, including the purpose for which the system is in operation and the identity of the data controller. This is achieved by having a documented CCTV policy and by placing easily read and well-lit signs in prominent positions.

5. Illegal Use of Enforced Subject Access Requests

Throughout 2016, the Office continued to find instances of inappropriate uses of subject access requests by organisations. It is unlawful for employers to require employees or applicants for employment to make a Section 4 access request to a data controller, such as An Garda Síochána seeking a copy of any personal data recorded about them, which is then made available to the employer or prospective employer.

6. Computer-System User Accounts

When an employee moves within or leaves an organisation, the access rights they have to the various computer systems must be amended or rescinded. Every organisation should have a written procedure in place in order to identify and disable lapsed system accounts. This is often called a 'movers, leavers and joiners policy'.

7. Security of Postal Arrangements

Ad hoc arrangements for delivering post and other documents to business reception areas can lead to security concerns. For example, a cardboard box used as a post drop and left in a reception area would not be considered secure. Postal correspondence being delivered to the lobby or reception area of an organisation should be kept securely out of sight of the general public. Other issues have also arisen in relation to organisations maintaining accurate and up-to-date addresses for customers.

8. Marketing

The collection and use of email addresses and mobile numbers for marketing purposes must be done in compliance with marketing regulations (SI 336 of 2011). Organisations must ensure that they have received the consent of the individual to receive marketing, and each communication must contain an unsubscribe option. Summary proceedings for an offence under SI 336 of 2011 may be brought and prosecuted by the Data Protection Commissioner.

In response to findings such as these, the audit team makes best-practice recommendations, gives immediate direction to an organisation to take a particular action or outlines a time frame during which rectifying measures should be taken.

Legal

Establishment of centralised internal legal function

2016 saw the establishment of a centralised legal unit within the DPC, through the recruitment of a senior solicitor with expertise in litigation and data protection as Head of Legal at Deputy Commissioner level. As part of our ongoing plan for the development of the DPC, the unit will be expanded over the next year as an element of our 2017 recruitment programme. While the centralised legal function will operate horizontally to provide support across all of our activities, a number of lawyers (solicitors and a barrister) amongst existing staff as well as staff with academic legal qualifications will continue to operate within all of our functional teams (investigations, audit, consultation). The centralised legal function will manage all forms of litigation in which the DPC is engaged and ensure a consistent interface with the legal teams in other EU data protection authorities in implementing the new harmonised GDPR law.

External legal advisors

In 2016, the Commissioner continued to be represented in litigation by, and receive external legal advice and services from, Philip Lee Solicitors, who were appointed on foot of an open tender process in 2015.

Launch of judgments database

As part of our ongoing drive to increase transparency and information available to the public on our activities, an online Judgments Database was launched on our website in December 2016. The objective of this project is to enable stakeholders and members of the public to directly access written judgments (including judgments which are not otherwise published online, i.e. Circuit Court judgments) in cases to which the Commissioner has been a party and to increase awareness of the developing national and European jurisprudence on data protection and privacy matters. This is an ongoing project and we will continue to collate judgments from past years and also to publish new judgments as they are delivered.

Criminal prosecutions

Prosecutions were taken by the Commissioner in 2016 for a range of offences committed under the Data Protection Acts 1988 & 2003 and under S.I. 336 of 2011 (often referred to as the “ePrivacy Regulations”).

A total of nine entities were prosecuted for offences relating to the rules on electronic marketing under the ePrivacy Regulations. Forty-five separate charges were brought across these nine sets of prosecutions. Details of the prosecutions are included in the Case Studies section (Appendix 2).

9 entities
prosecuted

for offences under Regulation 13 of S.I. 336 of 2011 in respect of electronic marketing. The summonses for these nine cases covered a total of forty-five offences.

Case Study 4

Prosecution of Yourtel Limited for Marketing Offences

We received a complaint in December 2014 from an individual who received marketing telephone calls from Yourtel Limited – a telephone service provider that had entered the Irish market in 2013 – after he had instructed the company during a previous call not to call him again. The complainant informed us that the calls related to an offer to switch telephone service providers.

In February 2015, a separate complaint was received on behalf of another individual who had received marketing telephone calls from Yourtel Limited after the company had been instructed during a similar marketing call on Christmas Eve 2014 not to call his number again. The marketing calls to this individual also concerned switching telephone service provider.

During our investigation of these complaints, Yourtel Limited acknowledged the making of the marketing telephone calls. It claimed that it had blocked the telephone numbers from receiving further marketing calls on the occasion of the last call in each case when it had been informed by the individuals concerned that they did not wish to be contacted again for marketing purposes. It did not accept in either case that it had continued to call the individuals after they had instructed Yourtel Limited not to call them again.

The Data Protection Commissioner decided to prosecute the offences as Yourtel Limited had come to our attention previously in 2014 on foot of a complaint about the making of a marketing telephone call to a telephone number that stood recorded on the National Directory Database (NDD) Opt-Out Register. Following the investigation of that complaint, we warned the company that it would likely face prosecution if it committed further offences under Regulation 13 of SI 336 of 2011 (known as the ePrivacy Regulations) at any future time.

At Dublin Metropolitan District Court on 21 January 2016, Yourtel Limited pleaded guilty to two charges of making unsolicited marketing telephone calls after the two individuals it called had notified the company that they did not consent to the receipt of such calls. The court convicted the company on both charges and it imposed two fines of €2,500 each. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

As regards prosecutions taken under the Data Protection Acts 1988 and 2003, one individual was prosecuted for offences under Section 22, one company was prosecuted for offences under both Sections 19(4) and 22 and a director of that company was prosecuted for offences under Section 29. These three prosecutions involved a total of 213 separate charges. Details of these prosecutions are set out in the section relating to our Special Investigations Unit and Appendix 2 Case Studies.

Statutory Enforcement Notices

Under Section 10 of the Data Protection Acts 1988 and 2003, where the DPC considers that there is or has been a contravention of the Acts, the DPC may issue an enforcement notice directing the person/entity concerned to take whatever steps are specified in the enforcement notice, within the time frame specified. Failure to comply with a requirement in an enforcement notice is an offence under the Acts for which the DPC can bring prosecution proceedings.

Details of the two enforcement notices that were issued by the DPC during 2016 are set out below. Enforcement notices are only issued where there has been a persistent failure by a person/entity to engage with the DPC and/or comply with a direction by the DPC. The vast majority of data controllers and processors voluntarily engage with us and comply with our directions without the DPC having to pursue formal enforcement action by issuing a statutory enforcement notice.

In the case of the enforcement notice at number 1 below, the data controller did not respond to the enforcement notice but ultimately complied with the matters specified in the enforcement notice following a subsequent warning that the DPC would commence prosecution proceedings against him if he failed to comply. In the case of the enforcement notice at number 2 below, the data controller did not respond to the enforcement notice and was warned that a prosecution would follow if there was no compliance. The data controller failed to respond and a prosecution was commenced against the data controller for failure to comply with the enforcement notice, by way of the issue of a District Court summons. Upon service of the summons, the data controller complied with the matters set out in the enforcement notice.

The District Court prosecution proceedings against the data controller were therefore struck out.

Enforcement Notices issued in 2016

| Data controller | Non-compliance issue |
|---|-------------------------------|
| 1. Joe Curran t/a Joe Curran Commercials, Oldcastle, Co Meath | Section 4(1) (access request) |
| 2. Antoinette McMahon, McMahon & Co. Solicitors, Woodquay, Galway | Section 4(1) (access request) |

Statutory Information Notices

Under Section 12 of the Data Protection Acts 1988 and 2003, the DPC may issue an information notice requiring a person/entity to provide in writing, within the time frame specified, the information specified that is necessary for the DPC to perform her functions. Failure to comply with an information notice, or the knowing provision of false or misleading information in response to an information notice, is an offence under the Acts for which the DPC can bring prosecution proceedings.

In 2016, a number of information notices were drafted in preparation for serving on various data controllers but none of those were ultimately required to be issued, as the data controllers concerned responded positively in all cases when they were advised that formal action by the DPC was imminent.

Statutory Appeals and Judicial Reviews

During 2016, the Commissioner was a respondent/defendant to the following sets of court proceedings:

An Appeal to the Supreme Court in the Case of Nowak v Data Protection Commissioner [2016] IESC 18 (Judgment Delivered on 28 April 2016 by O'Donnell J.)

This appeal was brought to the Supreme Court by the data subject who had been unsuccessful in his earlier appeals to the Circuit Court, the High Court and the Court of Appeal concerning the handling of his complaint by the Commissioner.

The Supreme Court considered the procedural question of whether there is a right of appeal under the Data Protection Acts 1988 and 2003 by a person who has made a complaint to the Commissioner but the Commissioner has decided not to investigate that complaint on the ground set out in Section 10(1)(b), i.e. where the Commissioner is ‘of the opinion that it is frivolous or vexatious’. The Supreme Court reversed the decisions of the Circuit Court, the High Court and the Court of Appeal on this question and found that in such circumstances there is a right of appeal against a decision by the Commissioner not to investigate the complaint.

The Supreme Court also considered the substantive data-protection-law question of whether an examination script for a professional accountancy examination (to which the appellant had sought access under an access request) was personal data within the meaning of the Data Protection Directive and the Data Protection Acts 1988 and 2003. The Commissioner had previously found that the examination script in question was not personal data and this had been upheld by each of the lower courts to which an appeal had been brought by the data subject. However, the Supreme Court found that this was ultimately a matter of European law and referred questions on the issue to the Court of Justice of the European Union for a preliminary ruling. This referral is still pending; the Court of Justice case reference for the referral is C-434/16.

A judicial review of the Commissioner’s decision not to hold an oral hearing in the case of *Martin v Data Protection Commissioner* [2016] IEHC 479 (judgment delivered on 10 August 2016 by Haughton J.)

This case involved an application for judicial review brought by a data subject who sought, among other things, an order of mandamus directing the Commissioner to conduct an oral hearing in order to resolve a conflict of evidence that had arisen in the course of an investigation into a complaint made by the data subject. While Haughton J. held that the application for judicial review was in fact moot due to certain procedural reasons, he expressed the court’s view on the substantive issue as to whether under the Data Protection Acts 1988 and 2003 or EU law the Commissioner has the power to conduct an oral hearing. In this regard, Haughton J. concluded that neither the Data Protection Acts 1988 and 2003 nor the Data Protection Directive expressly or by implication

require or empower the Commissioner to conduct an oral hearing in relation to complaints made under the Data Protection Acts. The court also held that the requirements of natural and constitutional justice do not confer an inherent power on the Commissioner to conduct an oral hearing even in circumstances where there is a factual dispute in relation to an alleged contravention of the Data Protection Acts. Haughton J. concluded that the data subject could have appealed the Commissioner’s decision to the Circuit Court and that the data controller, against whom the complaint was made, could have been joined as a notice party to that case. This process would have afforded the data subject an oral hearing and the resolution of the factual dispute at issue.

A statutory appeal against the Commissioner’s decision concerning a complaint in relation to an internet-search-result delisting request in the case of *Savage v Data Protection Commissioner*, Circuit Court, Record No. 2015/02589 (judgment delivered by Sheahan J. on 11 October 2016)

In this case, the data subject brought an appeal to the Circuit Court against the Commissioner’s decision on his complaint against Google. The complaint to the Commissioner arose from Google’s refusal of the data subject’s request to take down a link to a web page (for a discussion forum). The Commissioner’s decision was that there had been no contravention of the Data Protection Acts 1988 and 2003 as the link to the web page was accurate in that it represented an opinion of the data subject that was expressed by a user of the discussion forum, rather than a verified fact. The Circuit Court upheld the data subject’s appeal on the basis that the webpage link in question bore the appearance of a verified fact and that therefore it was not accurate because it was not clear from the link that the original poster was expressing their opinion.

Appeals have been taken to the High Court by both the Commissioner and by Google Ireland (who were a notice party to the original Circuit Court appeal). Those appeals are listed for hearing in May 2017.

Litigation Concerning Standard Contractual Clauses

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 an EU Commission decision, 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 that the CJEU has previously ruled (in its 6 October 2015 judgment, which also struck down the Safe Harbour EU-US personal-data transfer regime) must be followed by an EU data-protection authority where a complaint is made by a data subject that concerns an EU instrument.

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 unlawfully by US State security agencies. Mr Schrems’ concerns arose in light of the disclosures by Edward Snowden regarding a programme called ‘PRISM’, said to be operated by the US National Security Agency. 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 he was bound under existing national and EU law to apply that decision. Mr Schrems brought a judicial review action against the Commissioner’s decision and that action resulted in the Irish High Court making a reference to the CJEU.

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. 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 validity.

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, namely Article 7 (the right to respect for private and family life, home and communications), Article 8 (the right of every person to protection of their personal data) and 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 continues 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.

The Proceedings and 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. 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 that four of those ten parties (the US Government, BSA Business Software Alliance, Digital Europe and EPIC) be joined as amici.

The hearing of the proceedings before the Irish High Court (Commercial Division) took place over 21 days in February and March 2017. Judgment has been reserved and as of the time of going to print, no indication has been given as to when judgment will be delivered.

Challenge to the Independence of the DPC

High Court proceedings were commenced against the State and the Attorney General in November 2015 by Digital Rights Ireland Limited (DRI) claiming that the State is in breach of its EU law obligations by reason of the fact that the Commissioner is not an independent authority as required under the Data Protection Directive (Directive 95/46/EC). DRI are seeking various declarations by the High Court and, if necessary, a referral to the CJEU on certain specified questions arising from the claims made by DRI that the Commissioner is lacking in independence. The Commissioner has not been named as a party to these proceedings. The exchange of pleadings continued during 2016 and the Commissioner understands that the State is fully defending the claims made by DRI.

EU Legislative Developments

2016 saw extremely significant developments in the evolution of the EU data-protection legal framework, with the finalisation and adoption of two legal instruments designed to completely overhaul the existing EU-wide regulatory regime for data-protection. These are the General Data Protection Regulation and the Data Protection Directive for Police and Criminal Justice Authorities. General Data Protection Regulation (GDPR)

The finalised text of the GDPR (Regulation (EU) 2016/679) was published by the European Parliament and the Council of the EU on 27 April 2016. The GDPR will apply across all Member States of the EU from 25 May 2018 onwards. Simultaneous to the commencement of

the GDPR's application on 25 May 2018, the existing EU law on data protection, the Data Protection Directive (Directive 95/46/EC), will be repealed. The GDPR emphasises transparency, security and accountability by data controllers, while at the same time standardising and strengthening the right of European citizens to data privacy.

Data Protection Directive for Police and Criminal Justice Authorities

Processing of personal data for law-enforcement purposes is expressly excluded from the scope of the GDPR. However, in tandem with the adoption of GDPR, the European Parliament and Council have also adopted a Directive (Directive (EU) 2016/680) for the purposes of regulating the processing of personal data by law-enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data. The directive will also repeal Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. As a directive, this instrument requires transposition into national law. The transposition process by Member States is to be concluded by 6 May 2018.

Draft Electronic Privacy Regulation

As part of the EU's overhaul of the existing legal data-protection framework, a draft regulation setting out new rules on privacy in electronic communications was published on 10 January 2017 (COM/2017/010/final). The purpose of the draft regulation is to align the existing rules on privacy in electronic communications (currently set out Directive 2002/58/EC (as amended by Directive 2006/24/EC and Directive 2009/136/EC) and known as the ePrivacy Directive) with the GDPR. The draft regulation must progress through the EU legislation-making process but once the final text of the regulation is approved and published, it will repeal the existing ePrivacy Directive. The EU Commission has proposed that the new ePrivacy Regulation should have effect from 25 May 2018.

Engagement on GDPR Legislation

The GDPR is an EU regulation, which is a directly applicable legal instrument that is binding in its entirety and applies across the EU. As such, the GDPR directly addresses both organisations that process personal data, in terms of the obligations it imposes, and individuals, in terms of the rights that it confers upon them. While a regulation does not normally require domestic transposition in order to apply as the law in EU Member States, there are a number of provisions in the GDPR where Member States are permitted or required to exercise a limited margin of discretion as to the application of a particular provision. For that reason, national legislation to give effect to those articles is required. During 2016, the DPC, as a key stakeholder in the new regulatory regime under GDPR, engaged extensively with officials from the Department of Justice and Equality in relation to the preparation of the draft legislation, which will be required to give effect at a national level to the relevant articles of GDPR. That engagement remains ongoing.

EU/ US Instruments

Adoption of the Privacy Shield

A new framework for the transfer of personal data from the EU to the US, called Privacy Shield, was adopted by the European Commission on 12 July 2016 (by way of Commission Implementing decision (EU) 2016/1250) as the replacement to the Safe Harbour regime which was struck down by the CJEU on 6 October 2015.

EU/ US Umbrella Agreement

The EU/ US Umbrella Agreement which sets out a high level data protection framework for EU-US law enforcement co-operation was signed on 2 June 2016 and entered into force on 1 February 2017.

See Appendix 3 for data protection case law of the CJEU in 2016.

Binding corporate rules and Google common position application

Binding Corporate Rules (BCR) were introduced following discussions within the Article 29 Working Party in response to the need for organisations to have a global approach to data protection given that many consist of several subsidiaries located around the globe. As with the transfer of data on a large scale, it was recognised that this need must be met in an efficient way so as to avoid multiple signings of contracts such as standard contractual clauses or approvals by several DPAs.

During 2016, the DPC acted as lead reviewer in relation to seven BCR applications that will be finalised in 2017. We also acted as co-reviewer in four BCR applications, two of which, namely Starwoods and MasterCard, were approved in 2016. At the annual IAPP Europe Congress in Brussels in November 2016, the MasterCard BCR was used as a case study in a presentation by MasterCard's Managing Counsel to illustrate how smooth, swift and efficient the process was.

During 2016, we have also acted as lead reviewer for Google's WP 226 application, which involved an assessment of whether the terms of the Google-modified contracts were in line with standard contractual clauses for controller to processors adopted through an adequacy finding of the Commission in 2010. This was approved in 2016 – for G-Suite and Google Cloud. Although this was not a BCR application, it is an example of another cooperation procedure engaged in by the DPC with other EU DPAs.

It is envisaged that, with the recognition of BCRs as a tool to transfer data under the GDPR and the introduction of a one-stop-shop mechanism, there will be an increase in such applications and cooperation among EU DPAs.

During 2016, the DPC acted as lead reviewer in relation to seven BCR applications that will be finalised in 2017.

Guidance and Outreach

Promoting and building awareness of data-protection rights and obligations continued to be a key priority in 2016. Over the year, we proactively engaged in providing guidance and communicating our key messages, using a broad range of communications channels, techniques and platforms. These included conferences and speaking events; engagement with the media and social media; guidance; and information-awareness-raising campaigns.

GDPR Awareness Raising

In 2016 we took a lead role in driving awareness of the new legal regime, working in collaboration with other stakeholders where appropriate. In 2017, we will intensify our GDPR readiness drive, again in cooperation with relevant bodies, acknowledging that effective GDPR awareness raising will be a combined effort of the DPC, the government, practitioners, industry and professional representative bodies.

In November 2016, we published a GDPR readiness document, 'The GDPR and You', to guide organisations through the main provisions of the GDPR and the steps they should be taking to prepare for May 2018. Further GDPR guidance will be published over the course of 2017.

In 2016 and continuing into 2017, we have been contributing extensively to the EU Article 29 Working Party initiatives to prepare timely guidance that will interpret a number of the principles-based areas that GDPR introduces.

In 2017, we will be conducting a publicity campaign, using a variety of communications channels to target the broadest possible base of data subjects, data controllers and data processors, to ensure that awareness of the GDPR extends to all business sectors.

Speaking Engagements

In 2016, we maintained an extensive outreach schedule and actively engaged with a broad base of stakeholders. This involved the Commissioner, Deputy Commissioners and other staff speaking and giving presentations at seminars, conferences and to individual organisations, including public-sector bodies, on over 60 occasions during the year. Examples included:

- Irish Centre for European Law Privacy and Data Protection conference
- IAPP Global Privacy Summit (Washington DC)
- Public-sector GDPR awareness-raising seminar
- Websummit (Lisbon)
- PDP conference
- UCD Student Legal Convention 'Data Protection and IT Rights – The Right to Know and the Right to be Forgotten'
- Assistant Secretary Network Annual conference
- Data-protection breakfast briefings hosted by various law firms
- Irish Computer Society National Data Protection conference
- Datenschutz Kongress (Berlin)
- Institute of Banking seminar
- Sandyford Business District Association Data Protection seminar
- CSO-hosted UN conference on Big Data in Official Statistics
- Annual eHealth conference
- Presentation to interdepartmental committee on data sharing in the public sector
- Presentations to legal, international and digital marketing students at various universities and colleges

In addition to GDPR-related guidance, in 2016 detailed guidance was published on the following data-protection issues

Published Guidance

Data Sharing in the Public Sector

This guidance assists public-sector bodies in devising compliant data-sharing arrangements in light of the seminal CJEU decision in *Bara & Oths C-201/2014*. That judgment clarified a number of matters involving public-sector data-sharing arrangements such as the importance of adequately informing all data subjects in advance about the processing of their personal data. Adherence to our updated guidelines facilitates the lawful sharing of data between public-sector bodies. It is incumbent on all public-sector bodies to complete a full review of their obligations and arrangements on the basis of these guidelines for both current or future projects, where relevant, to ensure that those arrangements are fully compliant with the Data Protection Acts and the upcoming GDPR.

Anonymisation

When carried out effectively, anonymisation and pseudonymisation can be used to protect the privacy rights of individual data subjects and allow organisations to balance this right to privacy against their legitimate goals. While anonymisation has great potential as a strategy to reap the benefits of open data for individuals and society, case studies and research publications have shown how difficult it is to create a truly anonymous dataset while retaining as much of the underlying information as required for the task. Our guidelines will assist data controllers in assessing the nature of the data they hold and in applying such techniques in an effective manner.

Connected Toys

In 2016, concerns emerged regarding possible data-protection issues that might occur when children and parents use toys with microphones and cameras that have an ability to connect to the internet. Some of these toys connect to apps on smartphones or tablets, which might allow for the collection and recording of 'conversations' between the toy and the child. For some of these products the voice recordings are shared with other companies, and the toys' terms and conditions may allow for a child's conversations to be used as the basis for targeted advertising. We published guidance for parents to inform them of what they should look out for when considering purchasing such toys.

Location Data

Electronic devices such as smartphones record their location. The location data captured, especially data about the precise pattern of an individual's movements over time, can reveal very intimate details about that person's personal life. This type of data may be valuable to some organisations, as it can allow very specific targeting of services to particular individuals. However, this also poses serious risks to individual privacy, as well as risks that such data may be used to make decisions that adversely affect the individual to whom it relates. Data controllers have a responsibility to minimise the amount of data collected, processed and retained because of risks posed by linked location data. Our guidance assists organisations in finding out when the collection of location data is allowed and what their obligations are when collecting or processing such data.

General Election Canvassing and Direct Marketing

To assist candidates with protecting the individual's right to data privacy when canvassing in the 2016 general election, we published guidance on candidates' obligations in respect of the collection of the personal details of constituents and the use of electronic marketing to contact constituents.

Guidance on access requests, direct marketing and data-protection impact assessments will be published in the first half of 2017.

Social Media

In October 2016, we launched our Twitter account @DPCIreland, which we are proactively using to disseminate regular and key messages on our work, the GDPR and other important data-protection-related messages. In the five months following the launch, our tweets generated over 390,000 impressions and we have grown our national and international Twitter following to over 1,250.

New Website

Detailed planning for a new website progressed in 2016. We are currently preparing to commence a procurement process to award a contract for the development of the website. In particular, the new site will take account of GDPR requirements while facilitating the online notification of data breaches and notification of Data Protection Officers.

EU and International Engagement

Article 29 Working Party

In 2016, the Commissioner and/or Deputy Commissioners attended all plenary meetings of the Article 29 Working Party, which acts as an advisor to the European Commission on data-protection issues. It also promotes a uniform application of EU data-protection law throughout the European Economic Area. The main areas of focus of the Working Party in 2016 were preparing common positions and guidance on the application of the GDPR and matters relating to EU-US data transfers. In May 2018, the Working Party will become the European Data Protection Board in the new harmonised system brought about by the GDPR.

With the purpose of assisting the Article 29 Working Party in fulfilling its mandate, nine subgroups are active in areas such as technology, GDPR guidance and procedures, data transfers, law enforcement, financial matters, and cooperation between the data-protection authorities. In 2016, we actively participated in each of the groups, participating in some 50 meetings in Brussels throughout the year.

Our active role in the Article 29 Working Party structures means that we can share expertise and knowledge with our colleagues from across the EU on a broad range of issues, while also contributing to the consistent interpretation of European data-protection law and the drafting of opinions and guidance on the application of the law.

EU Joint Supervisory Bodies

During 2016, we continued to participate in the work programmes of the Joint Supervisory bodies of JSB Europol, Eurojust and JSA Customs and the European Data Protection Supervisory Groups for Eurodac and the Internal Market Information (IMI) database. By way of exercising our supervisory powers we conducted audits of Europol, Eurodac and the IMI.

EU TAIEX Programme

We also participated in two events under the EU Commission-sponsored TAIEX programme in 2016:

- TAIEX Workshop on protection of personal data in the social-welfare sector, Ankara, Turkey
- TAIEX Expert Mission on privacy in the employment relationship (workplace privacy and employee monitoring) organised in cooperation with Directorate for Personal Data Protection, Former Yugoslav Republic of Macedonia

International Cooperation

In addition to being an active participant at an EU level, the DPC proactively engages with the international data-protection community. The importance of protecting the personal data of individuals is a global imperative that can best be achieved when data-protection authorities worldwide share knowledge and good practice and, where appropriate, agree common positions on data-protection objectives and standards. In 2016, we continued to cooperate with our international DPA colleagues through the Global Privacy Enforcement Network (GPEN), our Memoranda of Understanding with other DPAs, and bi-lateral contacts.

As part of our engagement with other DPAs we attended a number of conferences, including:

- International Conference of Data Protection and Privacy Commissioners (Marrakech, Morocco)
- Spring Conference of European Data Protection Authorities (Budapest, Hungary)
- IAPP Global Privacy Summit (Washington, DC)
- British Irish and Islands' Data Protection Authorities Conference (Malta)
- IAPP Europe Data Protection Congress (Brussels)

During 2016 we also hosted representatives of the Canadian data-protection authority for discussions on issues of mutual interest – in particular, good-practice methodology in relation to investigations and audits.

GPEN Global Privacy Sweep – ‘Internet of Things’

In 2016, the Global Privacy Enforcement Network (GPEN) Privacy Sweep was conducted by 25 data-protection regulators around the world, including Ireland. The study looked at the ways in which companies operating in the Internet of Things communicated with their customers in regard to the security of their personal data.

This was the fourth annual GPEN sweep to be undertaken, following on from previous sweeps that examined online services for children, website privacy policies and mobile-phone apps.

The 2016 sweep found:

- **60%** of devices failed to adequately explain to customers how their personal information was collected, used and disclosed;
- **68%** failed to properly explain how information was stored;
- **72%** failed to explain how customers could delete their information from the device; and
- **38%** failed to include easily identifiable contact details if customers had privacy concerns.

Overall, the data-protection authorities examined more than 300 devices and are now considering action in respect of any devices or services thought to have been breaking data-protection laws.

In Ireland, the DPC investigated nine devices including smart electricity meters, telematics and fitness trackers. Our national findings were broadly in line with global trends. We subsequently carried out some follow-up work on the findings; following the GPEN sweep, we identified potential audit targets under each of these headings and our audit team has undertaken some initial investigative and scoping work. It is envisaged that an audit of one of these entities will take place in the first half of 2017.

The DPC investigated nine devices, including smart electricity meters, telematics and fitness trackers.

Registration

Certain categories of data controllers and processors are legally bound to register with the Data Protection Commissioner 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.

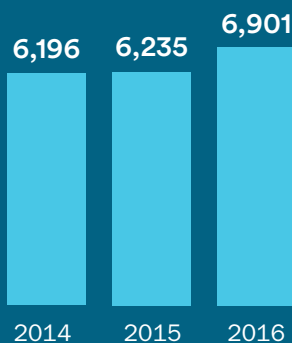
Registration should not be interpreted as automatically deeming an organisation to be fully data-protection-compliant by virtue of having their registration entry up to date. Data controllers, regardless of whether they are required to register, are bound by the data-protection responsibilities set out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

Registration is a legal requirement under current EU data-protection law, which will no longer be required under the General Data Protection Regulation from 25 May 2018. Transitional arrangements for 2018 are being developed in conjunction with the Department of Justice and Equality.

The total number of register entries in 2016 was 6,901.

| Category | Number |
|---|--------|
| Financial and credit institutions | 701 |
| Insurance organisations | 347 |
| Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts | 80 |
| Telecommunications/internet providers | 69 |
| Health sector | 2,417 |
| Pharmacists | 1,199 |
| Miscellaneous | 489 |
| Data processors | 1,599 |

Registration Entries 2014-2016



Corporate Affairs

Irish Language Scheme

The DPC's third Irish Language Scheme under the Official Languages Act 2003 commenced in October 2014 and remains in effect until October 2017. We continue to provide an Irish language service as well as Irish language information via our website www.cosantasonrai.ie.

Freedom of Information Act 2014

The DPC has been partially subject to the Freedom of Information (FOI) Act 2014 since 14th April 2015 in respect of records relating to the general administration of the office. Further information on making an FOI request to us can be found on our website www.dataprotection.ie. We also publish certain information on the office in accordance with Section 8 of the FOI Act under our Freedom of Information Publication Scheme which is also available on our website.

In 2016 we received a total of 20 requests referring to the FOI Act, compared with 9 in 2015.

An overview of these requests is provided as follows:

Of the 16 requests received in 2016 which were deemed to be outside the scope as the information sought did not relate to the general administration of the office, one was appealed by the requester to the Office of the Information Commissioner. In early 2017 the Information Commissioner affirmed the decision of the DPC.

Training

Our staff training programme continued in 2016. This included induction training and specialist data protection training for new and current staff, as well training in staff management, procurement, FOI and protected disclosures legislation. Of particular note, a two-day training course on the GDPR was provided to over 40 members of our staff. This was the first step in the process that will see a number of our staff obtaining an internationally recognised certification in data protection.

The Account of Income and Expenditure for 2016 is at Appendix 5 and the 2016 Energy Report at Appendix 6.

| Freedom of Information Requests Received by Type | Category Total | Outcome |
|--|----------------|----------------------|
| Relating to administrative issues | 1 | Refusal |
| Relating to personal data (outside of scope) | 3 | Refused/Not accepted |
| Relating to matters outside of the scope of the Acts | 16 | Refused/Not accepted |
| Overall Total | 20 | |

Appendices

Appendix 1

List of Organisations Audited or Inspected in 2016

The Commissioner would like to thank all of the organisations audited and inspected throughout the year for their cooperation. Although the inspection teams found that there was a reasonably high awareness of, and compliance with, data-protection principles in the organisations that were inspected, the majority required immediate remedial action in certain areas. Most demonstrated willingness to put procedures in place to ensure that they are meeting their data-protection responsibilities in full.

- National Transport Authority – taxi regulation
- Kilkenny NCT Centre
- Cavan General Hospital
- Laya Healthcare
- Vhi
- Allianz
- Residential Institutions Redress Board
- Europol
- ORAC/Eurodac
- An Garda Síochána – telecommunications data
- Defence Forces – telecommunications data
- Revenue Commissioners – telecommunications data
- Garda Ombudsman – telecommunications data
- Eir – (three inspections, including one for telecommunications data)
- Meteor – telecommunications data
- PeoplePoint
- Department of Defence (PeoplePoint)
- Department of Agriculture (PeoplePoint)
- Health and Safety Authority
- Internal Market Information (IMI) Database
- CPL Recruitment
- Paragon Executive Intelligence
- Pinergy
- Heatons CCTV
- Gamestop (credit-card sweep)
- Expert (credit-card sweep)
- Eleavon (credit-card sweep)
- AIB Merchant Banking (credit-card sweep)
- Dawn Foods
- Patrick Troy Solicitors
- Department of Social Protection
- Central Bank of Ireland
- Lawlor Partners
- Law Society of Ireland
- Two’s Company
- Eamon O’Mordha & Co. Ltd
- Surgical Symphysiotomy Payment Scheme
- KOD Lyons Solicitors
- NAMA
- Equality Tribunal
- Bank of Ireland
- Department of Education and Skills
- Dublin Tech Summit
- Grant Thornton
- Slane Credit Union
- Marks & Spencer CCTV (Liffey Valley)
- Marks & Spencer CCTV (Newbridge)
- Perfect Partners

Appendix 2

Case Studies

Case Study 1 – see section on Special Investigations

Case Study 2 – see section on Data Breach Notifications

Case study 3 – see section on Multinationals and Technology

Case study 4 – see section on Legal

Case Study 5 – Prosecution of Glen Collection Investments Limited and One of its Directors

The investigation in this case established that the defendant company obtained access to records held on computer databases in the Department of Social Protection over a lengthy period of time and that a company director used a family relative employed in the Department of Social Protection to access the records. The defendant company had been hired by a Dublin-based firm of solicitors to trace the current addresses of bank customers that the respective banks were interested in pursuing in relation to outstanding debts. Having obtained current-address information or confirmed existing addresses of the bank customers concerned from the records held by the Department of Social Protection, the defendant company submitted trace reports containing this information to the firm of solicitors that acted for the banks. The case came to light on foot of a complaint that we received in February 2015 from a customer of Allied Irish Bank (AIB), who alleged that an address associated with him, and that was known only to the Department of Social Protection, was disclosed by that department to an agent working on behalf of AIB.

The Data Protection Commissioner decided to prosecute both the company and the director in question, Mr Michael Ryan. Glen Collection Investments Limited was charged with 76 counts of breaches of the Data Protection Acts 1988 and 2003. Sixty-one charges related to breaches of Section 19(4) of the Data Protection Acts for processing personal data as a data processor while there was no entry recorded for the company in the public register, which is maintained by the Data Protection Commissioner under Section 16(2) of the Data Protection Acts. Fifteen charges related to breaches of Section 22 of the Data Protection 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.

Mr Michael Ryan, a director of Glen Collection Investments Limited, was separately charged with 76 counts of breaches of Section 29 of the Data Protection Acts 1988 and 2003 for his part in the offences committed by the company. This section provides for the prosecution of company directors where an offence by a company is proven 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.

The cases against Glen Collection Investments Limited and its director were called in Tuam District Court in January, May and July of 2016 before the defendants eventually entered guilty pleas on 10 October 2016. While the defendant company was legally represented in court on all occasions, the court issued a bench warrant for the arrest of the company director, Mr Ryan, on 10 May 2016 after he had twice failed to appear. The bench warrant was executed at Tuam District Court on 10 October 2016 prior to the commencement of that day's proceedings.

At Tuam District Court on 10 October 2016, Glen Collection Investments Limited pleaded guilty to 25 sample charges – 13 in relation to offences under Section 22 and 12 in relation to offences under Section 19(4). The company was convicted on the first five counts with the remainder taken into consideration. The court imposed five fines of €500 each. Mr Ryan pleaded guilty to 10 sample charges under Section 29. He was convicted on all 10 charges and the court imposed 10 fines of €500 each. In summary, the total amount imposed in relation to this prosecution was €7,500.

Case Study 6 – Prosecution of Shop Direct Ireland Limited T/A Littlewoods Ireland for Marketing Offences

In January 2015, we received a complaint against Shop Direct Ireland Limited T/A Littlewoods Ireland from an individual who had received an unsolicited marketing email after she had opted out of marketing from the company. The individual, who was a customer of Littlewoods Ireland, complained further a few weeks later when she received a marketing email promoting offers for Mother's Day from Littlewoods Ireland. We had previously issued a warning to Littlewoods Ireland in December 2014 following the investigation of a complaint received from the same complainant with regard to unsolicited marketing emails that she had received after she had opted out of receiving marketing. That previous complaint led to an investigation which found that the customer had not been given the opportunity to opt out of marketing from Littlewoods when she had opened her account. (She had been given the opportunity to opt out of third-party marketing only – an option to which she herself availed of). Arising from our investigation of that complaint, Littlewoods Ireland informed us that the customer's email address was opted out of direct marketing from 7 March 2014.

During the investigation of the 2015 complaints, the solicitors acting for Littlewoods Ireland informed us that, following the conclusion of the previous complaint in December 2014, Littlewoods Ireland had carried out a review of the customer's account. It found that while she was correctly opted out of email marketing, she was not opted out of third-party marketing. It then took steps to opt the customer out of third-party marketing. When the update to the third-party marketing preference was applied to the customer's account in January 2015 a null value was applied to the email marketing field. The intention in applying this null value was to signify that no change was to be made to this field. However, the application of this value had the unintended consequence of opting the customer back into email marketing. Subsequently, as a result of this incorrect update, two marketing emails were sent to the customer in January 2015 and March 2015.

The Data Protection Commissioner decided to prosecute the company. At Dublin Metropolitan District Court on 4 April 2016, Shop Direct Ireland Limited T/A Littlewoods Ireland pleaded guilty to one charge of sending an unsolicited marketing email without consent. The court ordered the payment of €5,000 in the form of a charitable donation to Pieta House and it adjourned the matter for seven weeks. 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 charge.

Case Study 7 – Further Processing of an Individual's Personal Data in an Incompatible Manner

An individual submitted a complaint regarding the unfair processing of their personal data. The individual stated that they had received letters from Thornton's Recycling and Oxigen Environmental respectively, explaining that there would be a change-over of refuse collection services from Oxigen Environmental to Thornton's Recycling within a week of the issuing of the letters. The complainant advised that they had not authorised the transfer of their personal details and had not been previously informed of this transfer of ownership.

We raised the matter with Oxigen Environmental, requesting an explanation as to the reason for processing personal data in this manner in light of the data-protection requirements of fair obtaining and fair processing of personal data. Oxigen Environmental confirmed that the customer details that were transferred to Thornton's consisted of a name, address and any balance that remained on the customer's pre-paid account. It advised that no banking details were passed over at any stage. It also alleged that a letter had been sent out to all customers advising them of the transfer and that this letter had been issued before any customer data had been transferred but they were not able to clarify the date on which this had allegedly occurred.

Oxigen Environmental indicated that the first and only notification that customers received regarding the transfer of services from Oxigen Environmental to Thornton's Recycling was made by way of two letters, one each from Oxigen Environmental and Thornton's Recycling, contained in the same envelope delivered to customers. The interval between this notification and the transfer of services spanned less than four working days. We considered that this was an insufficient time frame for customers to consider the change-over and to make alternative arrangements to prevent the further processing of personal data. While the issue of takeovers/mergers is often covered by a company's contractual terms with its customers, we established that Oxigen Environmental's terms and conditions and Customer Charter did not cover such issues.

Taking into account the short time frame that had elapsed between the notification of the transfer of services and the date from which the transfer became effective, our view was that the fair-processing requirements under the Acts were not fulfilled. While a proposal for amicable resolution was put forward, we were unable to conclude an amicable resolution of the complaint and a formal decision of the Commissioner issued in July 2016. The Commissioner found Oxigen Environmental to be in contravention of Section 2(1)(a) of the Data Protection Acts 1988 and 2003 in that it unfairly processed personal data without sufficient notice to its customers.

The requirement to provide proper notice of processing to data subjects in accordance with Section 2(1)(a) and Section 2D of the Data Protection Acts 1988 and 2003 is an essential pre-requisite to the lawful processing of personal data. A data subject has the right to be properly informed with adequate notice of a change in the ownership of a business holding his or her personal data, so as to be able to withdraw from the services being provided and prevent the further processing of their personal data (including preventing the transfer to a new owner) and to make alternative arrangements. The issue of what constitutes adequate notice will vary from case to case but, in any event, it must be at minimum a sufficient period that will allow a data subject to have a meaningful opportunity to consider the changes contemplated and to take steps to exercise their preferences in relation to the proposed changes.

Case Study 8 – Disclosure of Personal Information to a Third Party by a Data Processor

We received a complaint concerning the alleged unauthorised disclosure of the complainant's personal information by An Post to a third party. The complainant, who had recently been bereaved, informed us that An Post had erroneously issued a valuation statement in respect of a joint savings deposit account that they had previously held with their late partner to a solicitor acting on behalf of their late partner's son. The statement contained the complainant's personal financial data in relation to their joint State Savings account held with the National Treasury Management Agency (NTMA). Prior to making the complaint to this Office, the complainant had received an apology from An Post, on behalf of the NTMA, who acknowledged that the complainant's personal information had been disclosed in error. However, because the complainant had received very little information as to how the disclosure had occurred they requested that we investigate this matter.

Although the complainant submitted a complaint against An Post, we established in our preliminary enquiries that An Post offers products and services on behalf of State Savings, which is the brand name used by the NTMA to describe the range of savings products offered by the NTMA to personal savers. An Post is therefore a 'data processor' as defined under the Data Protection Acts 1988 and 2003 as it processes customers' personal data on behalf of the NTMA. The NTMA is the 'data controller', as defined under the Data Protection Acts 1988 and 2003, as it controls the content and use of its customers' personal data for the purposes of managing their State Savings account.

We commenced an investigation by writing to the NTMA, which did not contest the fact that the complainant's personal information had been disclosed. The NTMA stated that, having received a full report from its data processor, An Post, it had confirmed that, contrary to State Savings standard operating procedures, a valuation statement, which included details of an account held jointly by the complainant and their deceased partner,

was sent to a solicitor acting on behalf of a third party. The NTMA acknowledged that the information should not have been sent to the third party and that correct procedures were not followed in this instance by the data processor.

The complainant chose not to accept the amicable resolution of their data-protection complaint proposed by the NTMA, opting instead to seek a formal decision of the Data Protection Commissioner.

A decision of the Data Protection Commissioner issued in July 2016. In her decision, the Commissioner formed the opinion that the NTMA contravened Section 2A(1) of the Data Protection Acts 1988 and 2003 by processing the complainant's personal information without their consent by way of the disclosure, by An Post as an agent of the NTMA, of the complainant's personal information to a third party.

This case illustrates that it is vital for data controllers to ensure that their policies and procedures for the protection of personal data are properly and routinely adhered to by all staff. Staff awareness is key to this issue but employers should also ensure that regular reviews of how those policies and procedures are applied in practice are carried out so as to identify potential issues and enable the taking of appropriate remedial actions/ changes to the practices, policies and procedures.

Case Study 9 – The Necessity to Give Clear Notice When Collecting Biometric Data at a Point of Entry

In October 2015, we received a complaint from a contractor in relation to the alleged unfair obtaining and processing of their personal data. The complainant stated that in the course of attending a data centre for work-related purposes the company had collected their biometric data without their consent and had also retained their passport until they had departed from the data centre. While the complainant had been advised in advance by the data controller to bring identification on the day of attendance at the data centre for security purposes, they had not been informed at that time that the data controller would be collecting their biometric data upon arrival at the data centre.

In the course of our investigation, we established that the data controller had collected the complainant's biometric data upon their arrival at the data centre by way of a fingerprint scan. However, no information about this process had been provided to the complainant at that time – they were simply told that they could not go through security without this biometric fingerprinting. The data controller confirmed to us that this fingerprint-scan data had not been retained; rather it had been used to generate a numerical template that was then stored in encrypted form and that numerical information was associated with a temporary access badge provided to the complainant for the duration of the time in which the complainant was in attendance at the data centre. The data controller confirmed that it had deleted this

information from its system and the back-up files at the data subject's request upon the data subject's departure from the data centre. The data controller further confirmed that while it had retained the complainant's passport for the duration of the complainant's attendance at the data centre pursuant to a policy to ensure the return of temporary access badges, it had not taken or retained a copy of the complainant's passport.

The complainant in this case did not wish to accept the offer of amicable resolution made by the data controller and instead requested that the Commissioner make a formal decision on their complaint.

The decision by the Data Protection Commissioner in October 2016 found that the data controller contravened Section 2(1)(a) and Section 2D(1) of the Data Protection Acts 1988 and 2003 as the data controller should have supplied the complainant with the purposes of the collection and processing of the biometric data, the period for which it would be held and the manner in which it would be retained, used and, if applicable disclosed to third parties. This could have been done by the data controller either when it was in contact with the complainant to advise them of the requirement to bring identification to gain entry to the data centre, or at the latest, at the time the complainant arrived at the data centre.

However, in relation to the obtaining and processing of the complainant's biometric data, having reviewed the information provided by the data controller in the course of the investigation by this Office, the Data Protection Commissioner found that the data controller had a legitimate interest under Section 2A(1)(d) of the Acts in implementing appropriate security procedures for the purposes of safeguarding the security of data centre, in particular for the purposes of regulating and controlling access by third parties to the data centre. Given that the biometric data was used solely for the purposes of access at the data centre, it was not transferred to any other party and was deleted in its entirety at the data subject's request upon departing the data centre, the Data Protection Commissioner's view was that this did not amount to potential prejudice that outweighed the legitimate interests of the data controller in protecting the integrity of the data centre and preventing unauthorised access to it. Accordingly, the Data Protection Commissioner concluded that the data controller had a legal basis for processing the complainant's biometric data.

In relation to the retention of the complainant's passport for the duration of their visit at the data centre, the Commissioner found that this did not give rise to any contravention of the Data Protection Acts 1988 and 2003, as the data controller had a legitimate interest in doing so and the limited processing of the complainant's passport information (i.e. the retention of the passport itself) did not give rise to any disproportionate interference with the complainant's fundamental rights.

Transparency is a key principle under data-protection law

and the giving of notice of processing of personal data to a data subject is a major element of demonstrating compliance with this principle. In particular, the central tenet that individuals whose data is collected and processed should not generally be surprised by the collection and processing, or its scale or scope, should inform all aspects of a data controller's data-processing operations.

Case Study 10 – Residential Care Home's Legitimate Use of Audio Recording and Photograph of Data Subject Concerning Allegations of Misconduct

We received a complaint from a former employee of a residential care home who claimed that photographic evidence and an audio recording of them were used in a disciplinary case against them by their employer resulting in their dismissal.

During our investigation, the complainant's former employer (the operators of the residential care home) advised us that a formal, externally led investigation had been conducted into allegations that the complainant had been found by a supervisor to be asleep during a night shift on two separate occasions. On the nights in question, the complainant had been the sole staff member on duty responsible for the care of a number of highly vulnerable and dependent adults who had complex medical and care needs and who needed to be checked regularly. Having discovered the complainant asleep on the first occasion, the supervisor had warned the complainant that if it happened again it would be reported in line with the employer's grievance and disciplinary procedure. On the second occasion, when the supervisor discovered the complainant to be asleep, fully covered by a duvet on a recliner with the lights in the room dimmed and the television off, the supervisor had used their personal phone to take photographs of the complainant sleeping and make a sound recording of the complainant snoring. The allegations had been upheld by the investigation team and a report prepared. This was followed by a disciplinary hearing convened by the employer. The employer had informed the complainant at that hearing that it accepted the verbal and written account given by the supervisor. The employer had found that the act of sleeping on duty constituted gross misconduct in light of the vulnerabilities and dependencies of the clients in the complainant's care and the complainant had been dismissed.

Having regard to the information supplied to us by the operators of the residential care home and, in particular, the vulnerability of the clients involved and the nature of the complainant's duties, we formed the view that no breach of the Data Protection Acts 1988 and 2003 had occurred. In this case, we considered that the processing of the complainant's data, by way of the photograph and audio recording made by the supervisor, and the subsequent disclosure of these to the employer was necessary for the purposes of the legitimate interests

pursued by the data controller, the employer, under Section 2A(1)(d) of the Data Protection Acts 1988 and 2003. This legal basis for processing requires the balancing of the data controller's (or a third party's or parties') legitimate interests against the fundamental rights and freedoms or legitimate interests of the data subject, including an evaluation of any prejudice caused to those rights of the data subject.

We considered that the processing of personal data here was limited in nature and scope as it consisted of a one-off taking of a photograph and the making of an audio recording by the supervisor, who acted of their own volition and not in response to any direction or request from the employer. There had been limited further disclosure of the personal data concerned afterwards, i.e. to the employer, while the original photograph and recording were deleted from the supervisor's phone. A copy of the material had also been provided to the complainant in advance of the complainant meeting the investigation team. We therefore considered that, in the circumstances, the processing was proportionate and that the legitimate interests of the data controller (and indeed the legitimate interests of third parties, being the clients of the residential care home) outweighed the complainant's right to protection of their personal data.

While the right to protection of one's personal data attracts statutory protection within the national legal system and, moreover, is a fundamental right under EU law, such rights are not absolute. Accordingly, they must be interpreted to allow a fair balance to be struck between the various rights guaranteed by the EU legal order. In particular, as this case demonstrates, data-protection rights should not be used to 'trump' the rights of particularly vulnerable members of society or the legitimate interests pursued by those organisations responsible for safeguarding the health and life of such persons in discharging their duties of care and protection.

Case Study 11 – Disclosure of Personal Information to a Third Party

We received two complaints from public servants (a husband and wife) whose personal data was disclosed by PeoplePoint, the human resources and pension shared services for public-service employees. The initial complainant, in November 2015, stated that after applying for annual leave, he subsequently made an application to change this request to sick leave. The officer in PeoplePoint responsible for this section proceeded to email the complainant's line manager at the government department in which the complainant worked. However, on receiving an out-of-office reply the officer proceeded to email the complainant's non-supervisory peer. PeoplePoint had notified us of the breach in June 2015. However, on commencing an investigation and receiving a copy of the email at the centre of the breach, we established that the personal data of the complainant's spouse, who was also a public servant in a different department, was also contained

in the email and that the email had been sent to three third parties. It became apparent that the official in PeoplePoint, when considering the initial complainant's annual leave, had also accessed his spouse's personal information without the authorisation of her employer or her consent.

On further investigation into this matter it became apparent that the PeoplePoint official had informed the complainant's spouse and their colleagues about information in relation to the complainant when they had no legal basis to do so and without any authority from the data controller of their personal data, i.e. the employer.

PeoplePoint was subject to an audit by the DPC. In relation to this complaint, it informed us that upon being made aware of the breach, it acted to retrieve the data and confirmed that the data had been deleted by all parties involved. It also stated that corrective action had been taken to improve the relevant official's awareness of data privacy. While a proposal for amicable resolution was proposed by PeoplePoint, the complainants declined it and requested a formal decision of the Commissioner.

The Commissioner concluded the opinion that Section 21(1) of the Data Protection Acts 1988 and 2003 had been contravened. PeoplePoint is a processor engaged by the data controller (being the relevant government department, which is the employer) and as such the data processor owes a duty of care to the data subjects whose personal data it is processing. Under Section 21, a data processor must not disclose personal data without the prior authority of the data controller on behalf of whom the data are processed.

This case is a stark reminder to data processors of the importance of processing data only with the prior consent of the data subject or the data controller. Actions in relation to personal data that may appear innocuous to ill-informed staff can have serious ramifications for data subjects. It is not acceptable for data processors and data controllers to rely on an excuse that an employee did not realise that what they were doing was a breach of data-protection law. It is the responsibility of such employers to ensure that all staff are appropriately trained and supervised in relation to the processing of personal data, in order to minimise, to the greatest degree possible, the risks to the fundamental rights and freedoms of data subjects whose personal data they process.

Case Study 12 – Failure of Data Controller to Keep Individual's Personal Information Accurate and Up to Date, Which Resulted in the Disclosure of Personal Data to a Third Party

We received a complaint in February 2015 concerning the alleged unauthorised disclosure by Permanent TSB (PTSB) of the data subject's personal information to a third party. In this complaint, the data subject stated that she had lived at a property with her ex-husband, that the mortgage for this property was a joint account

in both her and her ex-husband's names and that she was subsequently removed from this mortgage as part of a divorce settlement. The data subject informed the DPC that she subsequently took out a separate mortgage with PTSB, solely in her own name, for a different property. However, PTSB had sent a letter of demand addressed to her at her new property and addressed to a third-party property that she had never been associated with. The complainant's ex-husband had been raised at this property; his stepmother was still living there and she had opened the PTSB letter of demand and notified her stepson (the data subject's ex-husband), who in turn had notified the data subject. We commenced an investigation and PTSB accepted that the data subject's personal data had been disclosed to a third party. PTSB informed us that this had occurred because the third-party address (which the data subject had provided to PTSB as a correspondence address when applying for the previous loan, which she held with her ex-husband) was incorrectly linked to the entirely separate subsequent mortgage loan in the data subject's sole name.

We sought an amicable resolution of this complaint but the proposal that PTSB offered the data subject was declined and she instead sought a formal decision of the Commissioner.

The Commissioner found that PTSB had contravened both Section 2A(1) of the Data Protection Acts 1988 and 2003 by processing the data subject's personal data without her consent or another legitimate basis for doing so and also Section 2(1)(b) by failing to keep her personal data accurate, complete and up to date.

The circumstances of this complaint are a case in point as to the rationale behind the principle that personal data must be kept accurate, complete and up to date. Failure to adhere to this principle, particularly in the context of contact information, perpetuates the risk that further data-protection failures (such as unauthorised disclosure to third parties) will flow from such non-compliance.

Case Study 13 – Failure by BOI to Properly Verify the Identity of Individual on the Phone, Which Resulted in the Disclosure of Personal Information to a Third Party

We received a complaint that Bank of Ireland (BOI) had disclosed the complainant's personal information to a third party. BOI had notified the complainant of this disclosure, which occurred when, in an attempt to contact him regarding his account, a member of BOI staff called his mobile and did not get an answer. BOI stated that as the staff member could not contact him on his mobile, they then attempted to contact him via the landline number listed on his account. According to BOI's notification, the complainant's mother had answered the phone and the BOI advisor requested to speak with the complainant, who shares his name with his father, and explained to the complainant's

mother that they could not discuss the account with her as she was not listed on the account. By referring to the complainant by his last name, Mr X, his mother mistakenly thought the call was in relation to the account she held with her husband, who is also called Mr X. BOI's position was that the complainant's mother was adamant that she was listed on the account and therefore the advisor should speak to her about it. Certain information was then provided to the complainant's mother regarding his account.

We commenced the investigation of this complaint by writing to BOI, asking it to confirm if it had already reported this breach to us as is considered good practice under our Personal Data Security Code of Practice. BOI did not contest the fact that the complainant's personal data had been disclosed and it confirmed that the breach had been previously reported to us. BOI had indicated that some confusion had arisen, due to complainant's father having the same name as him and having a banking relationship with the same branch, and as a result of this confusion, BOI had failed to properly identify the person with whom it was dealing and disclosed the complainant's personal information to a third party. BOI claimed that it was only made aware of the disclosure of his personal information when the complainant's mother phoned the advisor later that day to inform BOI that the complainant was her son and that the information was in relation to his loan accounts. BOI also advised us that a letter of apology had been issued to the complainant.

The complainant in this case declined the offer of amicable resolution made by BOI and requested a formal decision of the Commissioner.

The Commissioner concluded in her June 2016 decision that BOI had contravened Section 2A(1) of the Data Protection Acts 1988 and 2003 when it processed the complainant's personal information without his consent by disclosing it to a third party.

This case is a further demonstration of how a simple failure by a staff member to rigorously adhere to the requirement to verify a data subject's identity before disclosing their personal data can result in unauthorised disclosure of personal data. While the circumstances of this case involved the verbal unauthorised disclosure of personal data to a family member of the data subject concerned, this in no way makes it any less serious than if it had been a written disclosure to an unrelated third party.

Case Study 14 – Data Controller Obligated to Demonstrate Effort Made to Locate Data Within the Statutory 40-day Period

We received a complaint from an individual concerning an access request that they had submitted to Meteor, seeking a copy of their personal data and, in particular, the call recordings of calls they had made to Meteor Customer Care for a particular period. Meteor responded initially to his request by stating that only 10% of calls to its customer-care line are recorded and retained for 30 days and that there was no guarantee that his calls from the previous 30 days had been recorded. Meteor subsequently replied to the complainant's access request definitively, stating that there were no calls recorded and available in relation to the complainant.

We commenced an investigation of the complaint requesting information from Meteor in relation to the efforts it had undertaken to retrieve the call recordings that were the subject of the access request as well as information on the locations and/or business units to which enquiries were made in relation to the requester's access request. Meteor supplied us with a printout showing the searches undertaken and it responded that it did not hold any calls in relation to the complainant.

In this case, the issue of compliance with the 40 days for responding to an access request under the Data Protection Acts 1988 and 2003 was at issue. The complainant had made a valid access request to Meteor by email dated 24 August 2015. Meteor had finally responded to the requester by email on 29 October 2015 with a substantive answer. This substantive response to the access request fell nearly four weeks outside the 40-day statutory period for responding. Furthermore, Meteor did not provide us with any evidence that it had commenced the search for the call recordings that the complainant had sought within that 40-day period but instead chose to rely on its policy that only 10% of customer-care-line calls are recorded and simply assumed that the complainant's calls had not been recorded.

Despite attempting to amicably resolve this complaint, we were unable to do so and the data subject requested a formal decision from the Data Protection Commissioner. In her decision, the Data Protection Commissioner concluded that Meteor had contravened the Data Protection Acts 1988 and 2003 by not responding to the complainant's access request within the 40-day period as provided for under Section 4(1)(a).

This case demonstrates that a data controller must not approach a valid data access request on a simple assumption that it does not hold the personal data that is sought. Irrespective of the circumstances of the request, any policies employed or assumptions held by a data controller, it must take all steps necessary to establish in fact whether the requested data is, or is not, held by the data controller and to respond substantively to the access request within the 40-day statutory

period. The right of access of a data subject is one of the cornerstones of the protection of an individual's personal data and this right must not be stymied by the actions of data controllers, whether unintentional or otherwise.

Case Study 15 – Personal Data Withheld from an Access Request by Airbnb on the Basis of an Opinion Given in Confidence

We received a complaint in July 2016 from an individual (an Airbnb guest) concerning an access request that he had submitted to Airbnb. The essence of the complaint was that Airbnb had not provided the guest with a particular email about him that had been sent to Airbnb by the host of the Airbnb accommodation that the guest had rented. That email related to a complaint by the host about the guest. In responding to the guest's access request, Airbnb had withheld this email on the basis that it consisted of an expression of opinion given in confidence by the host.

Of relevance here was Section 4(4A)(a) of the Data Protection Acts 1988 and 2003, which allows for personal data that consists of an expression of opinion about the data subject by another person to be disclosed by the data controller to the data subject in response to an access request without the need to obtain the consent of the person who gave the opinion. Equally relevant was Section 4(4A)(b)(ii) of the Data Protection Acts 1988 and 2003, which provides for an exemption from the right of access to personal data where the personal data consists of the expression of an opinion about the data subject by another person that has been given in confidence or on the understanding that it could be treated as confidential.

We commenced an investigation that examined in particular whether the email in question from the host to the data controller, Airbnb, consisted of the expression of a confidential opinion by the host about the guest. We found that the content of the email in question was predominately factual in nature. While one element of the email comprised an expression of opinion, there was no reference or indication in the email to an expectation on the part of the host that the contents of the email would be kept confidential or not disclosed by Airbnb to the guest. In fact, we noted that in another email directly from the host to the guest, the host had indicated to the guest that they had contacted Airbnb about the guest.

While Airbnb was clearly trying to fairly balance the rights of the guest against the rights of the host in this case, it was our view, based on our examination of the issues and communications involved, that there was no evidence at all of an expectation or understanding by the host that their email about the guest would not be released to him. In those circumstances no exemption from the right of access applied under Section 4(4A)(b)(ii). Airbnb accepted our position and accordingly

released the email in question to the guest. This allowed the complaint to be amicably resolved.

As this case demonstrates, before withholding personal data on the basis that it consists of the expression of an opinion given in confidence or on the understanding that it could be treated as confidential, a data controller must ensure that there is a solid basis for such an assertion. It is not enough for a data controller to simply assume that this is the case in the absence of any indication to this effect from the person who expresses the opinion.

Furthermore, the inclusion of an opinion that attracts this exemption does not mean that all other personal data that is contained within the same document is similarly exempt from the right of access. Rather, in the context of a full document of personal data, the data subject is entitled to access the personal data within it that is not an opinion given in confidence and the data controller may only redact the part or parts to which the exemption validly applies. Opinions about individuals in respect of which no expectation of confidentiality can be shown to apply, or indeed information that is simply confidential, are not exempt from an access request.

As outlined in our published guidance, an opinion given in confidence on the understanding that it will be kept confidential must satisfy a high threshold of confidentiality. Simply placing the word 'confidential' at the top of the page, for example, will not automatically render the data confidential. In considering the purported application of this exemption to a right of access, we will examine the data and its context and will need to be satisfied that the data would not otherwise have been given but for this understanding of confidentiality.

Case Study 16 – Crypto-ransomware Attack on a Primary School

In October 2016, we received a breach report from a primary school that had been the victim of a crypto-ransomware attack, whereby parts of the school's information systems had been encrypted by a third party thereby rendering the school's files inaccessible. These files contained personal details including names, dates of birth and Personal Public Service Numbers (PPSNs). A ransom was demanded from the school to release the encrypted files.

Our assessment of the attack identified that the school had deficiencies in the measures it had taken to secure pupils' personal data, including:

- no policies or procedures were in place to maintain adequate backups;
- no procedures or policy documents existed focusing on system attacks such as ransomware or viruses;
- no contracts with data processors (the ICT services providers) were in place (as is required under Section 2C(3) of the Data Protection Acts 1988 and 2003) setting out their obligations and, as a result,

actions taken by the ICT suppliers were inadequate in response to the attack; and

- a lack of staff training and awareness of the risks associated with opening unknown email attachments or files.

We considered that the school had contravened the provisions of Section 2(1)(d) of the Acts, having failed to ensure that adequate security measures were in place, to protect against the unauthorised processing and disclosure of personal data.

Recommendations were issued to the school that it take steps to mitigate the risks identified. The school subsequently informed us that it had taken the following steps based on the recommendations issued, which were:

- Implement a staff training and awareness programme on the risks associated with email and the use of personal USB keys.
- Implementation of a contract-review process to ensure appropriate contracts are in place with its ICT suppliers.
- Ensure that any ICT support the school engages with either on a local basis or as recommended by the School Board is performed by competent data processors.

This case demonstrates that schools, like any other organisation – commercial, public sector or private – operating electronic data-storage systems and interacting online must ensure that they have appropriate technical security and organisational measures in place to prevent loss of personal data, and to ensure that they can restore data in the event of crypto-ransomware attacks.

Case Study 17 – Data Breach at an Online Retailer

In July 2016, we received a breach report from an organisation operating retail and online sales. The organisation had been notified by a customer that their credit card was used in a fraudulent transaction without their knowledge, which they believed arose from their provision of payment details online to the organisation.

The organisation engaged an expert third party to conduct an analysis of its website. It was determined that the payments system on the website had been compromised by malware for the previous 6–8 weeks. The malware copied data entered by customers during the online payment stage to an external destination.

Our assessment of the breach identified that there were deficiencies in the measures that the organisation had taken to secure users' personal data, including the following:

- No contract or service-level agreement existed between the data controller and the data processor.
- No steps were taken to ensure that the data processor was compliant with technical security and organisational measures.
- Insufficient measures were in place relating to appropriate technical security and organisational security measures to:
 - ensure that the server and website platform were maintained and that the software versions were up to date;
 - ensure that appropriate user authentication and access control measures were in place;
 - ensure appropriate technical security was in place, such as secure configuration of the website platform, measures to detect malware, measures to monitor suspicious activity and measures to ensure regular backups were taken; and
 - ensure governance processes were in place such as periodic reviews of the data processor and its technical security and organisational measures.
- that appropriate security measures are in place;
- that reasonable steps are taken to ensure that employees of the data controller and any other persons – for example, data-processor employees – associated with the processing are aware of their obligations;
- that proper contractual agreements are in place governing the processing;
- that reasonable steps are taken to ensure compliance with the measures.

Case Study 18 – Incorrect Association of an Individual’s Personal Details with Another File

We received a complaint concerning an alleged breach of an individual’s data-protection rights by an insurance company.

During our investigation, the insurer (Insurer X) advised us that the complainant had in the past requested a quotation for household insurance from another insurance company (Insurer Y), the undertakings of which had been transferred to Insurer X. Insurer Y had failed to delete the quotation (the complainant had never proceeded to take out a policy) in line with its own data-retention policy. In addition, Insurer Y had mistakenly linked the complainant’s personal details on the quotation to an insurance-claim file in respect of a claim it had received from a person with an identical name.

When a transfer of Insurer Y’s undertakings to Insurer X was being completed, the insurance-claim file that mistakenly included the complainant as the claimant (rather than another individual who had the same name) was transferred to Insurer X. The claim when assessed later turned out to be fraudulent and Insurer X had its solicitors write to the complainant, advising that their claim was found to be fraudulent and indicating the follow-up action that Insurer X intended to pursue to protect its interests.

At its centre, this case concerned sloppy handling of personal data. Many people in Ireland have the same name and there was no reason why the complainant’s personal details, collected when the complainant obtained a quotation, should have been added to an insurance-claim file. Sufficient checks and balances should have existed in Insurer Y’s data-handling processes. However, the more significant issue that arose for this complainant is that they were unable to ascertain, prior to our involvement, how their details came to be in the possession of Insurer X and how the issue that arose had come about.

A number of contraventions therefore occurred in this case – a breach of the requirement of a reasonable retention period due to holding onto the quotation data longer than necessary and longer than was set out in the company’s own retention policy; unlawful further

In light of the above, we considered that the organisation had contravened Section 2(1)(d) of the Data Protection Acts 1988 and 2003 by failing to take appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure or destruction of, its users’ personal data.

Recommendations were issued to the organisation that it take steps to mitigate the risks identified. The organisation subsequently informed us that it had taken the following steps to address the recommendations:

- Contracts are now in place to ensure that the appropriate technical security and organisational measures are in operation;
- The organisation conducts regular reviews of the server and website platforms to ensure that they are maintained and that the software versions are up to date;
- The organisation conducts annual reviews by a third-party expert to ensure compliance and to independently validate that the appropriate technical security and organisational measures are in place.

This case highlights the need for organisations to ensure that they have appropriate technical security and organisational measures for ICT security in place, particularly when engaging a data processor. Organisations should be cognisant of the measures outlined under Section 2C of the Acts to understand their obligations, in particular to ensure:

processing of the personal data by associating it with a claim file; failure to respond in a clear and timely manner to the complainant to explain how their data had been sourced and how it came to be processed in the way that it was. The complainant in this case suffered particularly serious consequences as they incurred significant legal costs in defending the accusation of making a fraudulent claim and the threat by Insurer X of instigating Circuit Court proceedings against them.

Case Study 19 – Prosecution of The Irish Times Limited for Marketing Offences

On 28 April 2015, we received a complaint from an individual who had received an unsolicited marketing email earlier that day from The Irish Times Limited in the form of a Get Swimming newsletter. He explained that he had signed up for the Get Swimming newsletter some months previously and he told us that he had opted out after the receipt of the third or fourth issue by using the unsubscribe instruction at the bottom of the newsletter. However, he claimed that The Irish Times Limited continued to send him the Get Swimming newsletter each week thereafter and he continued to unsubscribe using the unsubscribe instruction. He informed us that he also emailed customer care in The Irish Times Limited on 21 April 2015, asking to be removed from the newsletter and warning that he would report the matter to the Data Protection Commissioner if this was not done. Customer Care responded on the same day, stating that they would remove him from the newsletter immediately. However, he received a further newsletter one week later.

In response to our investigation, The Irish Times Limited stated that this was a one-off issue that had arisen from a human error in configuring the unsubscribe process, which had subsequently been fixed. It confirmed that 64 other users had been affected. It informed us that a procedure had been put in place to prevent a recurrence.

The Data Protection Commissioner had previously issued a warning to The Irish Times Limited in November 2012 following the investigation of a complaint from a different individual in relation to marketing emails that he continued to receive after he had opted out of the receipt of such emails.

The Data Protection Commissioner decided to prosecute the company. At Dublin Metropolitan District Court on 4 April 2016, The Irish Times Limited pleaded guilty to one charge of sending an unsolicited marketing email without consent. The court ordered the payment of €3,000 in the form of a charitable donation to Pieta House and it adjourned the matter for seven weeks. 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 charge.

Case Study 20 – Prosecution of Coopers Marquees Limited for Marketing Offences

In September 2015, we received a complaint from an individual about a marketing email that she had received a few weeks earlier from Coopers Marquees Limited. The same individual had previously complained to us in January 2014 after she had received a marketing email from that company, which, she stated, she had not consented to receiving. During the course of our investigation of the first complaint, the company undertook to remove the individual's email address from its marketing database. We concluded that complaint by issuing a warning to the company that the Data Protection Commissioner would likely prosecute if it re-offended.

In response to our investigation of the second complaint, we were informed that a new marketing executive for the company had used an old version of the marketing database for a marketing campaign. This had resulted in the sending of the offending marketing email to the email address of the individual whose details had been removed for over a year. The company accepted that it did not have consent to contact the individual concerned by email and it claimed that there was human error on the part of the new staff member, which had caused the email to be sent. The Data Protection Commissioner decided to prosecute the company.

At Virginia District Court on 7 June 2016, Coopers Marquees Limited pleaded guilty to one charge of sending an unsolicited email without consent. The court ordered a contribution in the amount of €300 as a charitable donation to Mullagh Scout Troop and it indicated that it would apply the Probation of Offenders Act in lieu of a conviction. The defendant company agreed to make a contribution towards the prosecution costs of the Data Protection Commissioner.

Case Study 21 – Prosecution of Robert Lynch T/A The Energy Centre for Marketing Offences

In January 2015, two individuals complained to us about unsolicited marketing calls that they had received from The Energy Centre on their landline telephones. In the case of both complainants, their telephone numbers stood recorded on the National Directory Database (NDD) Opt-Out Register. In the case of the first complainant, he informed us that he had received an unsolicited marketing call on 5 January 2015 during which the caller offered to arrange to conduct a survey of his home for the purpose of recommending energy-saving initiatives that The Energy Centre could sell him. The complainant said that he told the caller not to call him again and he pointed out that his number was on the NDD Opt-Out Register. Three days later, the complainant had received a further unsolicited marketing call from The Energy Centre. In the case of the second complainant, he had received an unsolicited marketing phone call on 23 January 2015 from a caller from The Energy Centre who told him that there were sales agents

in his area and that she wished to book an appointment for one of them to visit his home. The same complainant had previously complained to us in November 2013, having received an unsolicited marketing phone call from the same entity at that time. His first complaint was amicably resolved when he received a letter of apology, a goodwill gesture and an assurance that steps had been taken to ensure that he would not receive any further marketing calls.

By way of explanation during the course of our investigation of the two complaints received in January 2015, The Energy Centre indicated that its IT expert had examined the matter and concluded that there was human error somewhere along the line when someone had transferred some telephone numbers from a non-contact list back into the to-be-contacted system.

The Data Protection Commissioner had previously issued a warning to The Energy Centre following the investigation of a complaint from a different individual in relation to unsolicited marketing calls that he had received on his landline telephone while his number was recorded on the NDD Opt-Out Register.

The Data Protection Commissioner decided to prosecute. At Drogheda District Court on 21 June 2016, Robert Lynch T/A The Energy Centre pleaded guilty to three charges of making unsolicited marketing telephone calls to the telephone numbers of two individuals whose numbers were recorded on the NDD Opt-Out Register. In relation to the first case, where the complainant's number was called on two occasions three days apart, the court convicted the defendant in respect of the charge for the second telephone call and applied a fine of €100; it took the other charge in relation to the first telephone call into account. In relation to the second case, the court applied the Probation of Offenders Act in respect of that charge. The defendant agreed to pay the prosecution costs incurred by the Data Protection Commissioner.

Case Study 22 – Prosecution of Paddy Power Betfair Public Limited Company for Marketing Offences

In June 2016, an individual complained to us about marketing text messages he was receiving from Paddy Power Betfair plc and he also alleged that the 'stop' command at the end of the text messages was not working. He stated that he had never placed a bet with Paddy Power Betfair plc but he recalled having used its Wi-Fi once.

During our investigation of this case, the company, in relation to the allegation that the 'stop' command was not working, admitted that there were technical issues with the opt-out service of its text provider and stated that it had acted immediately to rectify this once it had become aware of it. On the matter of marketing consent, the company informed our investigation that the complainant had logged onto the Wi-Fi at its Lower Baggot Street, Dublin, outlet in April 2016. It described

how a user must enter their mobile-phone number on the sign-in page, after which they receive a PIN to their phone that enables the user to proceed. After entering the PIN correctly, the customer is presented with a tick box to accept the terms of service, which includes a privacy policy. Having examined the matter, we advised Paddy Power Betfair plc that we did not see any evidence that the user was given an opportunity to opt out of marketing as is required by SI 336 of 2011 (the ePrivacy Regulations). We formed the view that the company was unable to demonstrate that the complainant unambiguously consented to the receipt of marketing communications. The company understood our position and it undertook to work with its Wi-Fi providers to add the required marketing consent tick box on its registration page. It also immediately excluded all mobile-phone numbers acquired through the Wi-Fi portals from further marketing communications.

The Data Protection Commissioner decided to prosecute the company. A warning had previously been issued to the company in 2015 following the investigation of a complaint from a different individual who had continued to receive marketing text messages after opting out.

At Dublin Metropolitan District Court on 28 November 2016, Paddy Power Betfair plc pleaded guilty to one charge of sending an unsolicited marketing text message without consent and one charge of not providing the recipient with a valid means of opting out of the receipt of further marketing messages. In lieu of a conviction and fine, the court ordered the defendant to contribute €500 to the Simon Community by 12 December 2016 and it adjourned the matter for two weeks. The company agreed to discharge the prosecution costs incurred by 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 23 – Prosecution of Trailfinders Ireland Limited for Marketing Offences

A complaint was lodged with us in June 2016 by an individual who had received unsolicited marketing emails at that time from Trailfinders Ireland Limited despite having been informed previously that her email address had been removed from the company's marketing database in August 2015. In its response to our investigation, the company acknowledged that the offending emails had been sent in error. It explained that it had received a written communication about a customer-care issue from the complainant a few days prior to the sending of the marketing emails and that its customer-care team had updated her case concerning that particular issue. This update triggered an automated process that inserted the complainant's email address into its marketing database. Trailfinders Ireland Limited apologised for the system error and it said that it should not have happened in any circumstances.

On foot of a previous complaint in 2015 against Trailfinders Ireland Limited from the same complainant concerning unsolicited marketing emails to which she had not consented, the Data Protection Commissioner had issued a warning to the company in January 2016. Following our investigation of the second complaint, the Data Protection Commissioner decided to prosecute the company.

At Dublin Metropolitan District Court on 28 November 2016, Trailfinders Ireland Limited pleaded guilty to two charges of sending unsolicited marketing emails without consent. In lieu of a conviction and fine, the court ordered the defendant to contribute €500 to the Simon Community by 12 December 2016 and it adjourned the matter for two weeks. The company agreed to discharge the prosecution costs incurred by 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 24 – Prosecution of Topaz (Local Fuels) Limited for Marketing Offences

In July 2016, an individual complained to us about an unsolicited marketing telephone call that he had received on his mobile telephone from Topaz (Local Fuels) Limited. He had previously complained to us in November 2015 about marketing text messages that the company had sent him without his consent and he informed us that despite attempting to opt out by replying ‘Stop’ he continued to receive more text messages. In its response to our first investigation, the company said that the inclusion of the complainant’s mobile telephone number in its promotional campaign was a result of a human error and it acknowledged the failure of its system to register his opt-out attempts. It informed us in February 2016 that it had removed the mobile-phone number concerned from its marketing database. We concluded that complaint at the time with a warning to Topaz (Local Fuels) Limited.

On receipt of the second complaint, we commenced a further investigation by seeking an explanation for the making of a marketing phone call to the individual’s mobile telephone in circumstances where we had previously been advised that the telephone number had been removed from the company’s marketing database. The company said that the number had been called by the call centre due to its presence on a list of leads/lapsed customers that was provided to the call centre by another area of the business. It stated that it had not gone far enough to ensure that a failure in its systems would not occur again in relation to this individual. It accepted that another marketing contact should not have happened in the absence of the individual’s consent. The Data Protection Commissioner decided to prosecute the company.

At Dublin Metropolitan District Court on 28 November 2016, Topaz (Local Fuels) Limited pleaded guilty to one charge of sending an unsolicited marketing text message without consent and one charge of not providing the recipient with a valid means of opting out of the receipt of further marketing messages. In lieu of a conviction and fine, the court ordered the defendant to contribute €500 to Our Lady’s Children’s Hospital, Crumlin, by 12 December 2016 and it adjourned the matter for two weeks. The company agreed to discharge the prosecution costs incurred by 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 25 – Prosecution of Dermaface Limited for Marketing Offences

In August 2016, we received a complaint from a former customer of Dermaface Limited after she had received an unsolicited marketing email. The complainant had previously been informed in 2014 on foot of a previous complaint about unsolicited marketing emails that Dermaface Limited had removed her details from its marketing list. Our investigation sought an explanation from Dermaface Limited. It informed us that the marketing email that was the subject of the latest complaint was sent through the clinic’s software system, which it had purchased. It claimed that the new system contacted patients and former patients who had previously been opted out of receiving marketing communications from it. It admitted that the complainant was one of those patients/former patients who had been sent a marketing email. It sent an apology to the complainant.

Following an investigation in 2011 of a complaint from a different individual who had received numerous marketing text messages from Dermaface Limited, the Data Protection Commissioner had issued a warning to the company. The Commissioner decided, therefore, to prosecute the company in respect of the latest offence.

At Dublin Metropolitan District Court on 28 November 2016, Dermaface Limited pleaded guilty to one charge of sending an unsolicited marketing email without consent. In lieu of a conviction and fine, the court ordered the defendant to contribute €300 to Our Lady’s Children’s Hospital, Crumlin, by 12 December 2016. The court also indicated that it expected the company to discharge the prosecution costs incurred by the Data Protection Commissioner and it adjourned the matter for two weeks. At the adjourned hearing the defendant produced proof of payment of the charitable donation and the Data Protection Commissioner’s costs. The court struck out the charge.

Appendix 3

Data-protection Case Law of the CJEU

There were a number of significant judgments delivered by the CJEU during 2016 and relating to data-protection law. These are summarised below.

VKI v Amazon EU – Case C-191/15 (Judgment Delivered 29 September 2016)

This case involved the question, among others, of which Member State law applies to processing of customer personal data by electronic commerce undertakings (i.e. online service providers) who are established in a Member State other than the one in which they are directing their activities/offering online services. The CJEU held that the processing of personal data by an undertaking engaged in electronic commerce would be governed by the law of the Member State to which that undertaking directed its activities but this was subject to it being shown (and it was for the national court to decide this) that the undertaking carried out the data processing in the context of the activities of an establishment situated in that Member State. On the issue of establishment, the CJEU stated that the absence of a branch/subsidiary in a Member State did not preclude such an undertaking from having an establishment there but that merely making its website accessible in a particular Member State did not constitute an establishment.

Breyer v Germany – Case C-582/14 (Judgment Delivered on 19 October 2016)

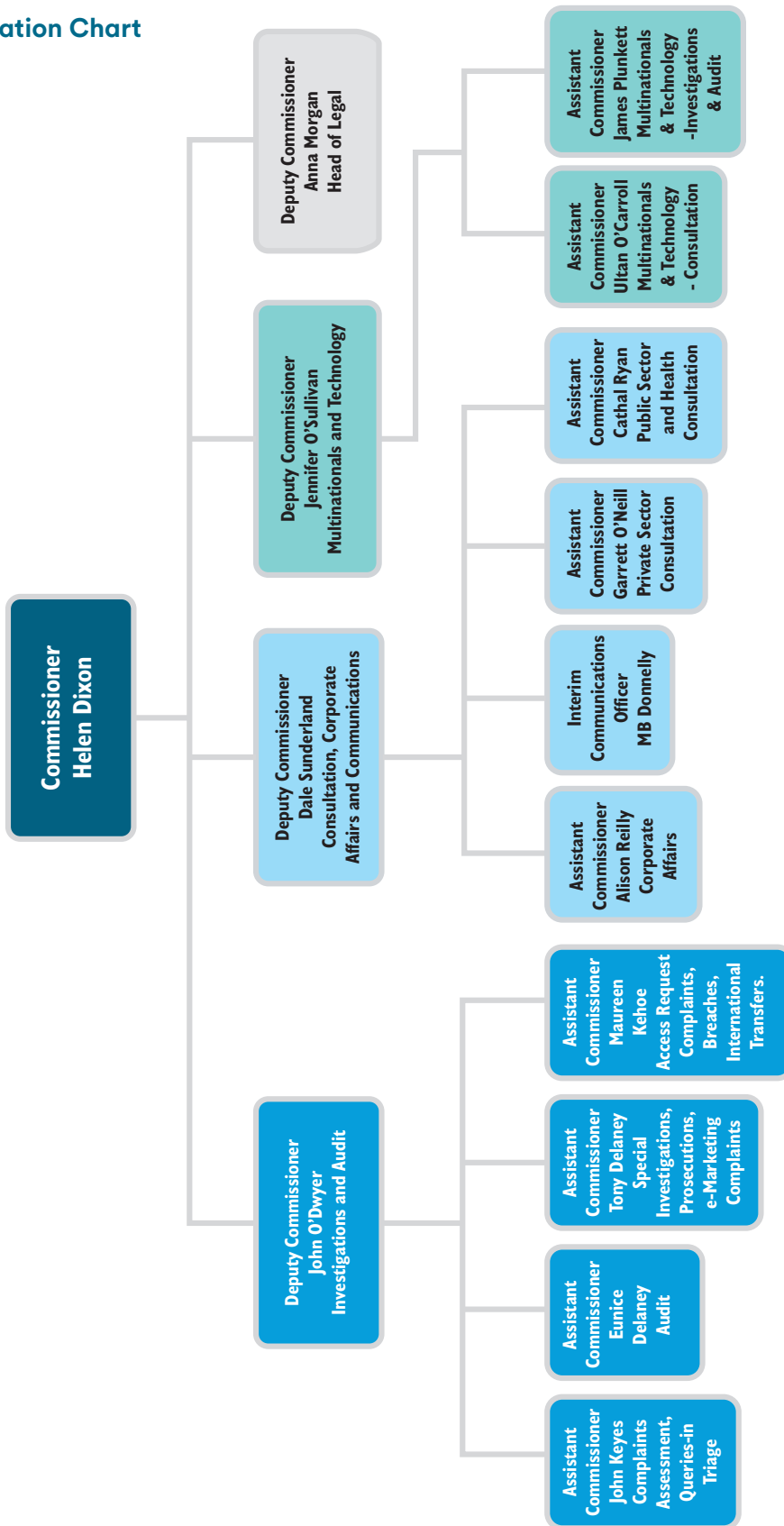
This case provided further guidance on what information may constitute personal data. Here the CJEU found that the dynamic IP address of a user, which is logged by the operator of a public website (in this case the websites were operated by German federal institutions) when the user visits the website, is personal data if the website operator can identify the user by legally requiring additional information on that user to be provided by the user's internet service provider.

Tele 2 Sverige v Swedish Post and Telecom Authority and Watson v UK – Joined Cases C-203/15 & C-698/15 (Judgment Delivered on 21 December 2016)

These joined cases concerned the legality of domestic legislative regimes in Member States (here, the UK and Sweden) that impose a general obligation on telecommunications operators to retain electronic communications data. The CJEU considered these in light of the CJEU's earlier (2014) ruling in the case of Digital Rights Ireland (Case C-293/12), the Charter of Fundamental Rights of the European Union and Directive 2002/58/EC, which establishes the general rule (and certain permitted exceptions to that rule) that traffic and location data should be erased or anonymised when no longer required for the transmission of a communication. The CJEU held that the effect of these measures was to preclude national legislation for the purpose of fighting crime that allows general and indiscriminate retention of traffic and location data of users relating to electronic communications. The CJEU also imposed a range of conditions significantly restricting the circumstances under which retention of such data, and access to such retained data, may be permissible. These include the requirements that: access to the retained data is subject to prior review by a court or independent body; notification of access to such data is made to the affected individual once such notification would no longer jeopardise an investigation; and the data is retained within the EU. Significantly the court also ruled that in light of the interference with fundamental rights that legislation allowing for the retention of and access to such data entailed, and given the requirement of proportionality in EU law, in the area of the prevention/investigation/detection/prosecution of criminal offences, only the objective of fighting serious crime was capable of justifying access to retained data.

Appendix 4

Organisation Chart



Appendix 5

Account of Income and Expenditure

Account of Receipts and Payments in the Year Ended 31 December 2016*

| Receipts | 2016 | 2015 |
|--|-------------------------|-------------------------|
| | € | € |
| Moneys provided by the Oireachtas | 3,905,588 | 2,963,107 |
| Fees | 775,729 | 670,307 |
| | <u>4,681,317</u> | <u>3,633,414</u> |
| Payments | | |
| Staff Costs | 2,540,891 | 1,989,204 |
| Establishment Costs | 340,495 | 283,396 |
| Legal and Professional Fees | 906,261 | 549,365 |
| Auditors fees | 10,200 | 4,600 |
| Miscellaneous Expenses | 107,741 | 136,542 |
| | <u>3,905,588</u> | <u>2,963,107</u> |
| Payment of receipts for the year to the Vote for the Office of the Minister for Justice and Equality | 747,225 | 648,073 |
| Receipts payable to the Vote for the Office of the Minister for Justice and Equality at year end | 28,504 | 22,234 |
| Total | <u>4,681,317</u> | <u>3,633,414</u> |

*The figures for 2016 outlined above are still subject to audit by the Comptroller and Auditor General. The final audited accounts will be presented to the Minister for Justice and Equality for presentation to the Oireachtas.

Appendix 6

Energy Report

Overview of Energy Usage in 2016

Dublin

The Dublin premises of the Office of the Data Protection Commissioner were temporarily based in the Regus Building, Harcourt Road, Dublin 2 from July 2015 to August 2016. The Dublin staff moved to dedicated premises in August 2016, based in 21 Fitzwilliam Square, Dublin 2. The energy rating details for the Dublin premises refer to 21 Fitzwilliam Square from August to December 2016. By the end of 2016, there were 25 members of staff accommodated in this building. In 2016, 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.

Portarlinton

The DPC's Portarlinton 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 2016, 27 members of staff were accommodated in this building. In 2016, the main use of energy in the Office was for gas and electricity for heating, lighting and other uses.

In 2016, the energy rating for the building in Portarlinton was C1.

Actions Undertaken

The DPC has participated in the SEAI online system in 2016 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 2016

Dublin Office

| Usage | |
|----------------|-----------|
| Non-electrical | N/A |
| Electrical | 36,480 kW |

Portarlinton Office

| Usage | |
|----------------|------------|
| Non-electrical | 46,629 kWh |
| Electrical | 51,650 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.

The GDPR and You

General Data Protection Regulation

An Coimisinéir
Cosanta Sonraí  Data Protection
Commissioner



1

Becoming Aware

Review and enhance your organisation's risk management processes – identify problem areas now.



2

Becoming Accountable

Make an inventory of all personal data you hold. Why do you hold it? Do you still need it? Is it safe?



5

How will Access Requests change?

Plan how you will handle requests within the new timescales – requests must be dealt with within one month.



4

Personal Privacy Rights

Ensure your procedures cover all the rights individuals are entitled to, including deletion and data portability.



3

Communicating with Staff and Service Users

Review all your data privacy notices and make sure you keep service users fully informed about how you use their data.



6

What we mean when we talk about a 'Legal Basis'

Are you relying on consent, legitimate interests or a legal enactment to collect and process the data? Do you meet the standards of the GDPR?



7

Using Customer Consent as grounds to process data

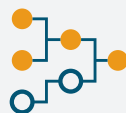
Review how you seek, obtain and record consent, and whether you need to make any changes to be GDPR ready.



8

Processing Children's Data

Do you have adequate systems in place to verify individual ages and gather consent from guardians?



10

Data Protection Impact Assessments (DPIA) and Data Protection by Design and Default

Data privacy needs to be at the heart of all future projects.



9

Reporting Data Breaches

Are you ready for mandatory breach reporting? Make sure you have the procedures in place to detect, report and investigate a data breach.



11

Data Protection Officers

Will you be required to designate a DPO? Make sure that it's someone who has the knowledge, support and authority to do the job effectively.



12

International Organisations and the GDPR

The GDPR includes a 'one-stop-shop' provision which will assist those data controllers whose companies operate in many member states. Identify where your Main Establishment is located in the EU in order to identify your Lead Supervisory Authority.

