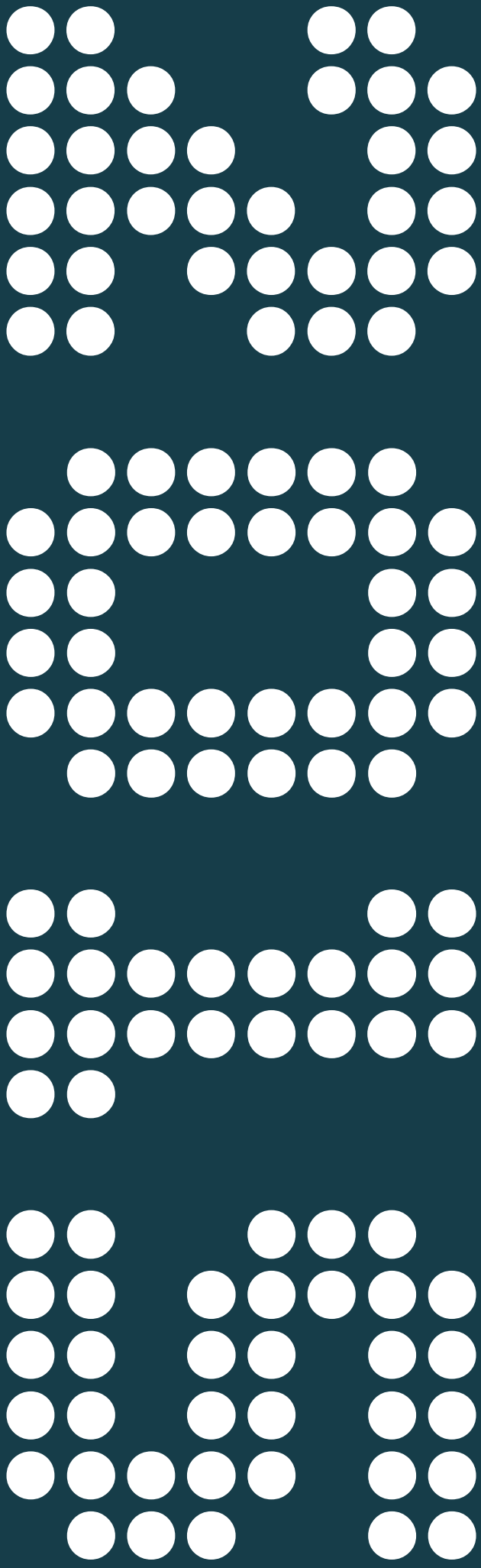
Annual Report of the Data Protection Commissioner of Ireland

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003



An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

TABLE OF CONTENTS

APPENDICES

HELEN DIXON
Data Protection
Commissioner of Ireland

FOREWORD

I'm delighted to present the 2015 Annual Report, an overview of the Office's activities in my first full year as Data Protection Commissioner of Ireland (DPC).

It has been a year of significant progress for the Office and for the protection of data rights at a domestic and international level, with fast-paced developments that are likely to prove far-reaching.

Continued Expansion

During 2015, the DPC continued the programme of building our capabilities and our capacity through significant recruitment including specialist legal, technical, investigatory and communications experts. A temporary Dublin premises on Harcourt Road now houses over 20 DPC staff, with the Dublin team moving to dedicated premises in the city centre in the second half of 2016. This new office expands our geographic reach, and works seamlessly with the existing 28 staff based in Portarlington, County Laois. As an authority with responsibility for protecting the data-privacy rights of users both in Ireland and, in many cases, across Europe, this continued drive to fully resource the significant role we are required to perform remains a key priority.

These increased resources and capabilities have allowed the authority to deliver clear improvements in response times, both for data subjects who raise complaints and for organisations seeking guidance in terms of implementing projects with implications for data-privacy rights. In 2015, the Office made substantial inroads into a legacy backlog, leading to an overall reduction in the number of open complaints. As required by statute, the Office achieved an amicable resolution between both parties in 94% of the investigations it concluded. But we also issued a record number of decisions under Section 10 of the Irish Data Protection Acts during 2015. CCTV in the workplace, direct marketing by SMS, email messages issued without consent, banks failing to keep personal contact information up to date, and non-responsiveness to data subject access requests appeared to be the issues that most occupied the public last year.

Consultation and Guidance

The numbers of requests for specific guidance by public- and private-sector organisations increased to 860, 120 of which were substantive consultations that required a number of meetings and contacts. Consultation with the DPC is not mandatory but many organisations seek guidance towards a compliant and privacy-enhanced service. Such consultations are often time-consuming but ultimately improve protection of the fundamental right to data privacy in the many cases where the DPC is able to make specific advance recommendations. An example is the case of the Mount Carmel Hospital Group liquidation, where the Office was able to provide advice in relation to the control and processing of personal medical data that was held by the hospital.

What becomes clear from dealing with many organisations in Ireland is that they deploy little resource themselves to manage data protection compliance. Some organisations appear to struggle with the principles-based nature of data protection legislation and suggest that it is difficult to correctly interpret and apply the principles in the specific scenarios with which they are dealing. From what I have seen, little real attempt is made in some cases to interpret and apply the principles and to examine

As society shapes the world we want to live in, data protection law must adapt and fit its safeguards around that shape.

implementation from the perspective of affected data subjects. In other cases, organisations appear to not even be conscious that what they are proposing represents a significant interference with an individual's data-privacy rights and view efficiency and cost-saving as automatically sufficient justifications for any action. The DPC remains committed to its role of providing specific guidance. It is vitally important in improving privacy outcomes. However, the DPC does not have the resources to replace the requirement for organisations to procure their own expert advice and to build their own capability to manage and drive compliance. It is helpful, therefore, that the forthcoming General Data Protection Regulation (GDPR) will bring an increased power of enforcement for data protection authorities, but, first and foremost, will explicitly put back onto organisations the clear obligation to properly organise themselves to ensure they are adequately protecting the individual's fundamental right to data privacy and can demonstrate their accountability in this regard. A question I am frequently asked at conferences is whether there is an inherent conflict between the role of the DPC in hearing complaints from individuals regarding potential contraventions of their data-privacy rights and the role of the Office in providing guidance to organisations. I believe no such conflict exists. Indeed, both roles are expressly prescribed in the EU legislation that underpins our functions, and, in fact, the GDPR will give greater emphasis to that consultation role, making it mandatory in certain cases. Additionally, while this Office and our European counterparts play an important role in advising the EU Commission on data protection matters, this does not bind us when it comes to examining a complaint from an individual. The provision of targeted guidance to organisations significantly improves privacy outcomes for individuals but never undermines the role of the Office in investigating a data protection complaint on its merits.

The provision of targeted guidance to organisations significantly improves privacy outcomes for individuals but never undermines the role of the Office in investigating a data protection complaint on its merits.

This is particularly the case where we engage with tech multinationals with bases in Ireland and are given advance preview of the global service changes that these corporations intend to implement. In many cases, this engagement is essential in protecting users' data privacy. For example, through consultation between Facebook and the DPC, Facebook delivered updated advertising settings and controls, a revamped Privacy Check-up tool and updates to the 'DYI' tool. An updated interface for user settings and the introduction of an access tool on LinkedIn arose from our engagement in 2015. However, the DPC, as is the case for all data protection authorities in Europe and globally, is still small relative to the span of the supervisory role assigned to us under national and EU legislation. Essentially, data protection authorities are the supervisors of **all** entities – public and private – and now increasingly individuals, too, where they act as data controllers. Prioritisation is therefore essential. Greater public debate and understanding of data privacy is also needed. As society shapes the world we want to live in, data protection law must adapt and fit its safeguards around that shape. In many ways, the bigger questions that need to be grappled with centre around the kind of world we want to live in, where the boundaries between man and machine should lie, and the balancing of power and responsibility between individuals and organisations. The work the DPC engages in through the Global Privacy Enforcement Network, the Article 29 Working Party and the International Conference of Data Protection Commissioners allows us to participate in expert discussions focused towards delivering the best outcomes for today's data subject, who is the subject of unprecedented personal-data collection, processing, tracking and profiling.

Queries, Complaints and Enforcement

The Office also dealt with many queries in 2015 about personal data in the public sector. A number of these arose in relation to the Eircode database – from individuals whose names were included alongside their Eircode and were available on the Eircode Finder. A limited number of queries were also received regarding incorrect spelling and allocation of townlands associated with Eircodes. Capita, the Postcode Management Licence Holder, worked with this Office to

develop a mechanism, in the format of a detailed Code of Practice and a set of FAQs, to help resolve these issues. The volume of queries the DPC received around this project underlines the extent of the testing required where personal data of individuals may be processed.

A small number of complaints were raised with the Office about the roll-out of the Department of Education's Primary Online Database, with issues cited around the legal basis for the collection and processing of the personal data involved, the quality of the information notices provided to parents, the use of the PPSN as an identifier in the database, and the purported linking of funding to schools with parents' compliance in providing their children's data. While some matters remain under ongoing investigation, it can only be emphasised again that strong analysis, risk identification and management, data protection impact assessment and effective communication are the foundations of any successful large-scale government data project.

It was a busy year for enforcement activity, with direct-marketing offences again to the fore in 2015, and the Office prosecuting a number of repeat offenders in relation to failures to implement opt-outs on text messages and failure to accurately record individuals' choice to opt out on their databases. The Office established a Special Investigations Unit headed up by an Assistant Commissioner to carry out investigations on its own initiative, as distinct from complaints-based investigations.

Awareness Building

Building awareness at a national level around data protection-compliance matters was also a strong focus this year and, together with my senior management, I undertook a very ambitious programme of speaking engagements across many industry sectors, speaking at 60 events. It was disappointing to be unable to deliver on the intended improvement to the presentation and comprehensiveness of guidance on the DPC website, but this is a priority currently under active delivery, with the results visible in mid-2016. Some of the expert staff and I completed a schedule of speaking engagements outside of Ireland in order to better communicate the role, work and outputs of the Office and in some cases to dispel fundamental misapprehensions as to purported differences between Irish data protection law and the regimes of other EU states. In particular, presentations by the Technology Advisor to the DPC at events such as the Future of Privacy Forum tech session at the International Conference of Data Protection Commissioners in Amsterdam in October, and our presence at the Digital Enlightenment Forum on ethics and technology, were very well received and allowed an interesting insight into the ways in which the Irish DPC is in effect shaping how large data companies are using and sharing personal data.

International

National and international matters merged in October last year when the Court of Justice of the European Union (CJEU) delivered its ruling in the case of Maximilian Schrems versus the Irish Data Protection Commissioner. The case was subsequently remitted to the Irish High Court, where the Irish Authority agreed to examine the complaint. This work is ongoing. The CJEU ruling was of major significance on a number of levels as it set out a new test based on German constitutional law in relation to the essence of the fundamental right; it reiterated its test for proportionality and necessity from the Digital Rights Ireland case on the Data Retention Directive; it clarified the role of data protection authorities in examining complaints even where the matter complained of is a binding EU instrument, and, of course, it struck down the Safe Harbour agreement itself.

The issue of EU–US transfers and, indeed, transfers of personal data from the EU to other global jurisdictions has occupied the Article 29 Working Party in particular since that ruling last October. The working party called for political intervention to create the necessary political and legal solutions to allow personal-data free-flows to continue in a way that also safeguarded the fundamental rights of European individuals. As of today, it remains to be seen whether the proposed Privacy Shield for EU–US transfers will represent the start of a solution.

The other major news in 2015 was the political agreement on a new legal framework for data protection in Europe after 4 years of negotiations. It comprises the new General Data Protection Regulation and a Directive to safeguard personal data processed in a law-enforcement context. The GDPR will bring new enumerated rights for data subjects in Europe, increase the obligations on organisations handling personal data, and bring a new enforcement focus to the role of data protection authorities. Importantly, as it is a harmonised law with direct effect in each EU member state, it will require Europe's independent data protection authorities to cooperate and work with each other in new ways in order to ensure its effective and consistent implementation to the benefit of data subjects and organisations alike. The clock is already ticking down to 25 May 2018 and my staff and I are preparing for our expanded role.

The Irish government also continued its commitment to data protection and increased public awareness of its importance through initiatives such as the Government Data Forum, chaired by the Minister of State with special responsibility for data protection, Dara Murphy, TD.

The past number of years have seen significant growth and strengthening of the Office, with a doubling of our staff and a near fourfold increase in our budget, backed up by a commitment from government that this increase in our resources will continue to keep pace with our responsibilities. This sees us in a stronger than ever position to continue to shape the data protection environment and ensure proper compliance with the relevant laws.

HELEN DIXON,
Portarlington and Dublin, 21 June 2016

ROLE AND RESPONSIBILITIES OF THE DATA PROTECTION COMMISSIONER OF IRELAND

Establishment, Roles and Responsibilities
The Office of the Data Protection Commissioner (DPC) is an independent body that derives its power and authority from the Data Protection Acts 1988 and 2003, which require the safe collection, storing and processing of individuals' personal information. Established in 1989, following the enactment of the Data Protection Act of 1988, the landscape facing the Office has dramatically changed with the growth of the internet and the exponential pace of technological innovation. With 9 out of 10 world-leading technology and internet companies as well as many of the world-leading pharmaceutical and financial-services firms now located here in Ireland, the range of issues we deal with has expanded greatly, as has our responsibility to Irish and EU service users. There are three main strands to our work; supervision, consultation and cooperation.

Supervision
This Office hears the complaints of individuals who believe that their data protection rights have been contravened. As obliged by Section 10 of the Act, we then seek to amicably resolve these complaints within a reasonable timeframe, and, where that proves not to be possible, to make a determination. This Office additionally conducts regular audits and inspections of organisations processing personal data where we identify risks through the complaints we receive. Details are set out on page 10. Where appropriate and provided for by legislation, we are empowered to act against organisations that commit offences under the Acts.

Consultation
We actively monitor the constantly changing landscape of data protection and provide up-to-date guidance to individuals and organisations. Undertaking regular and meaningful engagement with private and public organisations is key to this approach, seeking to ensure their compliance with data protection legislation in advance of the roll-out of a product, service, policy or business initiative.

Cooperation
Representatives of the Office are active participants in the Article 29 Working Party – an independent working party comprising the national data protection authorities in Europe (DPAs) – and focus on the protection of individuals rights with regard to the processing of personal data. Article 29 and its subgroups seek to harmonise the application of data protection rules throughout the EU, and each EU member state is represented at these important fora. Over the coming two years, the working party will develop into the European Data Protection Board in the new harmonised environment that will be brought about by the GDPR. The Office also participates in cooperation with our international DPA colleagues through the Global Privacy Enforcement Network (GPEN), our Memoranda of Understandings with other DPAs and bi-lateral contacts.

The DPC's role is set to expand and evolve under the GDPR, which was recently adopted and published in the *Official Journal of the European Union* on 4 May 2016. It will supersede EU Directive 95/EC/46. As 'lead supervisory authority' for the many multinational technology companies based here in Ireland, we will be required to cooperate (under the 'one-stop shop' mechanism) with our colleague DPAs across the EU. We will also acquire administrative fining capability for the first time. These matters, along with other new and expanded roles outlined in the GDPR, will require substantial preparation and resourcing.

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. The government has significantly increased funding to the DPC for 2016, and its annual budget now exceeds €4.7 million. The funding allocated in 2015 was €3.65 million.

While the DPC is an independent body, it ensures that oversight in relation to its administration follows the requirements set out for all public-sector organisations. All expenses, costs and expenditure must be accounted for to the exchequer, and the Office's accounts come under the Comptroller and Auditor General's remit. The daily interaction with citizens, businesses and other key stakeholders provides additional oversight of the work we undertake. Statutory decisions can be appealed to the courts.

The Data Protection Commissioner lists her current goals as being:

1. To continue to build the capacity and capability of the data protection authority in Ireland through the hiring of additional specialists, in particular with legal, technical and policy expertise.

2. To improve customer service and response times to individual complainants and organisations seeking guidance.

3. To ensure cohesion across the Portarlington- and Dublin-based operations of the DPC.

4. To continue to drive better compliance by public- and private-sector entities through the range of DPC supervisory activities.

5. To continue to build cooperative links with all stakeholders but in particular our A29 EU counterparts as we build towards implementation of the GDPR.

REVIEW OF 2015 IN BRIEF

- We dealt with 14,427 queries via our dedicated information email address, info@dataprotection.ie, an increase from 13,500 in 2014 and 12,000 in 2013. In addition, we dealt with 16,173 queries received by phone and 855 further queries by post.

- We received 932 complaints, which were opened for investigation. This compares with 960 complaints opened for investigation in 2014.

  The largest single category of complaints related to access rights, which accounted for over 60% of the total, reflecting the extent of the difficulties some individuals experience exercising their statutory right of access. The Office plans to conduct an awareness campaign highlighting these issues during 2016.

- The second-largest category of complaint concerned electronic direct marketing.

- While the majority of complaints were resolved amicably, we made formal decisions in 52 cases, 43 of which fully upheld the complaint.

- Following the CJEU decision in the 'Right to be Forgotten' case, we had 23 complaints, compared to 32 in 2014, regarding internet-search delisting.

- We prosecuted 4 entities for a total of 24 offences under the Privacy in Electronic Communications Regulations of 2011.

- While the vast majority of organisations engage voluntarily with us, we issued 3 Statutory Enforcement Notices.

- We received 2,376 data-security-breach notifications, an increase of 112 on the previous year.

- We carried out 51 audits and inspections including those on major holders of personal data in the public and private sectors.

- Notable audits included those of the Insurance Sector and Franchise Section, Dublin City Council.

- We engaged with large tech multinationals – with headquarters or a significant presence in Ireland – regarding numerous matters, including proposed new policies, products and services.

- The Commissioner or the Deputy Commissioner attended all plenary meetings of the Article 29 Working Party, which acts as an advisor to the European Union on data protection issues.

- We took part in the third Global Privacy Enforcement Network Privacy Sweep, analysing 18 apps and websites either targeted at or popular among children.

- Our running costs in 2015 were €2,961,190, an increase from €2,274,438 the previous year. Receipts for 2015 totalled €670,307.

- From 14 April 2015, the DPC became partially subject to the Freedom of Information Act 2014. This applies to administrative-matters records only, and specifically those created after 21 April 2008. DPC investigation and case files are not releasable under the Act.

- We dealt with over 500 queries from the media.

- We undertook significant recruitment, expanded the Office's Dublin base to complement the Portarlington function and virtually doubled our team.

- Extensive consultation across public- and private-sector bodies was undertaken, including participating in over 60 events where we presented the work of the Office.

- Utilising its increased resources, the Office established a Special Investigations Unit headed up by an Assistant Commissioner in 2015. The Unit carries out investigations on its own initiative (as distinct from complaints-based investigations); where it identifies offending behaviour, it will use the Commissioner's full range of statutory powers to progress its investigations to an appropriate conclusion.

- The hearing at the CJEU into Maximilian Schrems' complaint against the Irish DPC was heard in Luxembourg in March 2015. On 6 October, the CJEU issued its important and far-reaching ruling in the case, which included the striking-down of Safe Harbour.

  The Irish High Court remitted the matter for consideration to the DPC, which undertook to investigate '... the substance of the complaint with all due diligence'. The DPC commenced its investigation of the reformulated complaints submitted by Mr. Schrems. That investigation is ongoing.

- The GDPR was agreed in December 2015, applying from 25 May 2018. It will bring stricter breach-reporting obligations, the possibility of significant penalties in the case of compliance failures, greater focus on consent-based processing, more detailed record-keeping requirements alongside formal obligations to have a data-retention policy in place. Of major importance for the DPC is the GDPR's introduction of a 'one-stop shop' mechanism for multinationals operating in Europe. Given the scale and breadth of this constituency, the Office has an extremely important role in terms of global data protection.

CONTACTS, QUERIES AND COMPLAINTS

The DPC receives numerous contacts, queries and complaints on a daily basis. We operate an information email address (14,427 queries in 2015), an online complaints form (1,050 queries in 2015), a helpdesk (16,173 calls in 2015), and also receive queries by post (855 in 2015).

The Office makes every effort to progress and conclude each query, contact and complaint as effectively and efficiently as possible to the satisfaction of the querist.

Our Complaints Team is a core and busy function of the Office. In 2015, the team received 932 complaints that were opened for investigation, a small decrease on the 960 received in 2014.

Again, the largest single category of complaints related to access requests, accounting for 62% of the overall total for 2015, with 578 complaints topping the record high of 532 set in the previous year.

This continued high level of complaints indicates the increased awareness among the general public of their statutory right of access; however, perhaps of more concern, it also highlights the extent of the difficulties that some individuals experience trying to exercise those rights. The Office plans to conduct an awareness campaign highlighting these issues during 2016.

The second-highest category of complaints concerned electronic direct marketing. These complaints are investigated under the Privacy in Electronic Communications Regulations (SI 336 of 2011). In 2015, the Office opened 104 such complaints for investigation, 11% of the overall total. This is a sharp decrease of 72 complaints compared with the previous year, a trend that began in 2014 when, for the first time since 2005, complaints in this category dropped below 200 in a calendar year; this is indicative of the success of the Office's active prosecution strategy, which generates adverse publicity against entities prosecuted.

Right to be Forgotten

The so-called 'Right to be Forgotten' (RTBF) or internet-search-result delisting category of complaints emerged in 2014 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.

In November 2014, the Article 29 Working Party issued guidelines setting out a range of criteria to aid in the consistent assessment of cases – such as whether the individual plays a role in public life; whether the individual is a minor; whether the information is factually accurate; whether it relates to the private or professional life of the individual; whether it is up to date; whether it relates to sensitive personal data (such as about health or religion) or whether the individual made the information voluntarily public in the first place.

This Office received 23 such complaints in 2015 of which 7 were upheld and 16 were rejected.

One rejected complaint centred around a long-running tribunal, where the Office concurred with Google's position not to delist certain URLs found following a search conducted using an individual's name. Given that the individual concerned had given key testimony at this important tribunal, it was considered that there was a legitimate public interest in maintaining access to this information against a search on that individual's name. A search against other keywords in the original content would still have produced a result in the search engine.

Of the complaints that were upheld, one related to an interview given by an individual to a local newspaper 7 years previously regarding potholes on the local roads, which on a search of the individual's name was the first listed result. With the repairs to the potholes completed, the issue was resolved but the individual was unhappy that a search against their name still produced this story in the results. Arguing with Google on the complainant's behalf, we successfully made the case that the story was out of date and therefore no longer relevant.

Conclusion of Complaints

It is the statutory obligation of this Office to seek to amicably resolve complaints in the first instance and, accordingly, the vast majority of complaints concluded in 2015 were resolved amicably through the efforts of the Office without the need for a formal decision under Section 10 of the Act. In 2015, the Commissioner made a total of 52 formal decisions: 43 fully upheld the complaint, 1 partially upheld the complaint and 8 rejected the subject of the complaint. A total of 1,015 investigations of complaints were concluded in 2015.

Table 1
Breakdown of complaints opened, 2015
(See corresponding bar chart below)

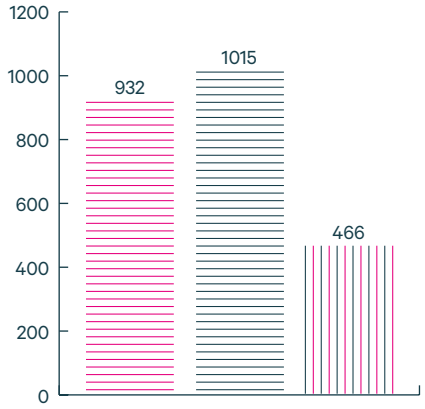
	Percentages	Totals
Access Rights	62%	578
Electronic Direct Marketing	11%	104
Disclosure	10%	94
Unfair Processing of Data	5%	49
Internet search-result delisting	2%	23
Use of CCTV Footage	2%	16
Failure to secure data	2%	16
Excessive data	2%	15
Right of rectification	1%	13
Accuracy	1%	10
Postal direct marketing	1%	7
Unfair processing of data	1%	5
Use of biometrics	<1%	2
TOTALS	**100%**	**932**

Table 2
Complaints received since 2006

Year	Complaints Received
2006	658
2007	1,037
2008	1,031
2009	914
2010	783
2011	1161
2012	1,349
2013	910
2014	960
2015	932

Table 3
2015

Complaints opened in year	932
Total complaints concluded in year	1,015
Total open complaints at end of year	466



Prosecutions

The Office prosecuted four entities in 2015 for a total of 24 offences under the Privacy and Electronic Communications Regulations (SI No. 336 of 2011). The Case Studies section carries further details of the prosecutions taken in 2015.

STATUTORY ENFORCEMENT NOTICES

Under Section 10 of the Data Protection Acts 1988 and 2003, the DPC may require a data controller or data processor to take whatever steps are considered appropriate to comply with the terms of the Acts.

Details of Statutory Enforcement Notices served in 2015 are set out in the following table. It is hoped that publication of these lists will encourage all organisations to cooperate fully with this Office in relation to its statutory investigations.

While an Enforcement Notice may be issued in relation to a number of aspects of the Data Protection Acts, it is not normally necessary to do so. The vast majority of organisations voluntarily engage with the Office without the need for a formal legal notice to advance an investigation.

Enforcement Notices issued in 2015:

Data controller:	In relation to:
Telefonica Ireland Limited	Section 2(1)(c)(iv) of the Data Protection Acts
Arizun Services Ireland Limited	Section 2(1)a and 2A(1) of the Data Protection Acts
Aer Lingus	Section 4(1) of the of the Data Protection Acts

INFORMATION NOTICES

Under Section 12 of the Data Protection Acts 1988 and 2003, the DPC may require a person to provide whatever information the DPC needs to carry out its functions, such as to pursue an investigation. In 2015, 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 of the fact that action by this Office was imminent. This is in line with the experience with other enforcement powers. Often, our communicating the potential for the use of such powers by the DPC is sufficient for the data controller to voluntarily engage, rather than risk the reputational damage of being named in our Annual Report or possibly incurring criminal sanctions for failure to comply.

DATA-BREACH NOTIFICATIONS

During 2015, the DPC received a total of 2,376 data-breach notifications of which 59 (2.5%) were classified as non-breaches under the provisions of the Personal Data Security Breach Code of Practice (PDSBCP).

A total of 2,317 valid data-security breaches were recorded during the period 1 January–31 December 2015. This represents an increase of 5.9% (129) on the number reported in 2014 (2,188).

Telecommunications and internet service providers have a legal obligation under Statutory Instrument 336 of 2011 to notify this Office 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 us 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 2015, a total of 104 data-breach notifications were received from the telecommunications sector, which accounted for 4.3% of total cases reported for the year. Examples of such breaches included SIM replacements carried out incorrectly, customers given online access to another customer's account and, in a small number of cases, customers' proof-of-identity documents were misplaced.

All other data-security breaches are reported under a voluntary PDSBCP, which was introduced in July 2011. The PDSBCP is not legally binding and does not apply to the telecommunications sector.

As in 2014, the highest category of data breaches reported under the PDSBCP were unauthorised disclosures such as postal and electronic disclosures, the majority of which occurred in the financial sector and accounted for just over 54% of total data-breach notifications received in 2015.

Typical examples of data breaches include:

- inappropriate handling or disclosure of personal data, e.g. improper disposal, third-party access to personal data – either manually or online – and unauthorised access by an employee;
- loss of personal data held on laptops, computers, USB keys, paper files and back-up tapes.

Although accounting for a small percentage of the 2,317 valid data-breach notifications in 2015 (3 or 0.12%), incidents of database hacking and website scraping can have far-reaching effects on individuals. In one case, customers of a Dublin flower shop had their credit-card details compromised. This was due to malicious codes being installed on the business website, which sent customer credit-card details to a third party. Once the shop became aware of the issue, they immediately arranged to take the credit-card payment system offline to facilitate enhanced security measures being implemented and also notified all customers who had made an online purchase in the previous 60 days.

Often, data controllers become aware of a data breach when they are contacted by an unaffected third-party recipient. Once aware of a data breach and, as per the provisions of the PDSBCP, the data controller then either seeks the return of the documents or requests confirmation from the third-party recipient that the documents have been destroyed. The data controller then contacts the affected individual, alerting them to the nature of the data compromised. This allows the individual to take whatever steps they believe appropriate to protect themselves. In the case of disclosure of financial information, the data controller may also put in place security measures to monitor activity on the affected individual's account to ensure that no fraudulent transactions can be carried out.

This Office is also often contacted by individuals who have received notification from a financial institution of a disclosure of their personal data. A common concern expressed in such cases is that they – the affected individuals – do not know who has received their personal financial information. However, data controllers cannot release the name and address of the third-party recipient, as to do so is a further breach of the Data Protection Acts. The data controller can only advise whether they have secured the return of the documents or have received confirmation that the documents have been destroyed.

It should be noted that, in case of the majority of personal-data breaches reported to this Office, only one or two individuals are impacted in each instance.

Upcoming Changes under the General Data Protection Regulation (GDPR)

Under Statutory Instrument 336 of 2011, only telecommunications and internet service providers currently have a legal obligation to notify this Office of a data-security breach. However, Articles 33 and 34 of the GDPR, which is due to come into effect in 2018, will legally oblige all data controllers to notify this Office of any personal-data security breach that occurs.

Article 33(1) of the GDPR states that 'the controller will without undue delay and, where feasible, not later than 72 hours after becoming aware of it, notify the personal data breach to the supervisory authority [...] unless the personal data breach is unlikely to result in a risk to the rights and freedom of natural persons'. It further states that, where the notification is not made within 72 hours, the data controller must provide reasons for the delay in reporting.

All such personal-data-breach notifications must include the following information:

- a description of the nature of the personal-data breach including, where possible, the number and category of data subjects affected and records concerned;
- contact details of either the data protection officer or other contact point;
- the likely consequences of the breach;

- measures taken or proposed to be taken to address the breach and, where appropriate, to mitigate its possible adverse effects.

Article 33 of the GDPR allows for the information listed above to be provided by the data controller to this Office in phases. However, it imposes a duty on the data controller to document the facts relating to, and the effects of, a personal-data breach and also the remedial actions taken. This will enable this Office to verify compliance with Article 33 with the relevant data controller.

With regard to the notification of a personal-data breach to affected individuals, Article 34(1) of the GDPR states that 'where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay'.

The tables below provide a breakdown of data-breach notifications received in 2015.

Table 1
Number of Breach Notifications Received, 2015

Total number of breach notifications received	2,376
Number considered as non-breach	59
Number of valid breach notifications	2,317

Table 2
Breach Notifications by Category and Type of Data Controller, 2015

Category	Public sector	Private sector
Theft of IT equipment	8	18
Website security	8	61
Unauthorised disclosure – postal	71	628
Unauthorised disclosure – electronic	169	270
Unauthorised disclosure – other	90	946
Security-related issues	12	36
Non-breach	40	19
Total	398	1,978

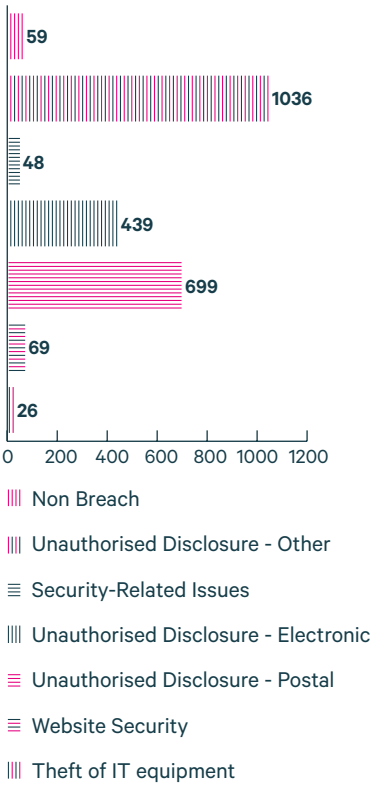
Table 3
Comparison of Breach Notifications, 2011–2015

Year	Number of valid breach notifications
2011	1,167
2012	1,592
2013	1,507
2014	2,188
2015	2,317

Table 4
Comparison of organisations making breach notifications, 2011–2015

Year	Private sector	Public sector	Total
2011	146	40	186
2012	220	84	304
2013	246	61	307
2014	254	60	314
2015	238	49	287

Breaches by Category



ENFORCED SUBJECT ACCESS REQUESTS

An 'Enforced Subject Access Request' is where someone is obliged by a potential employer or organisation to make an access request to a data controller under Section 4 of the Data Protection Acts. Section 4 gives individuals the right to obtain a copy of any information relating to them held by any entity or organisation; in an Enforced Subject Access Request, the individual is then required by the potential employer or organisation to provide this information to them. Typically, an enforced request entails an employer/prospective employer/recruitment agency requiring a person to make a request about themselves from organisations such as An Garda Síochána or credit bureaux.

Section 4(13) of the Data Protection Acts commenced in 2014 and, as a result, data controllers/data processors will now commit a criminal offence if they require individuals to make an access request in such circumstances.

This procedure is wholly different to the legitimate vetting of individuals for certain roles, such as child care, or those working in the private-security industry. The concern is that organisations who would not legitimately qualify to conduct a vetting check are instead turning to Section 4 of the Data Protection Acts to engage in 'vetting by the backdoor'. Worryingly, this request could potentially reveal a lot more sensitive data than a legitimate vetting check. A Section 4 access request could result in everything held on Garda records about a person being disclosed (subject to certain exemptions), chiefly because the data disclosed is intended to be for the information of the person making the request only. In contrast, a vetting check has always been subject to certain restrictions on what would be disclosed.

Cognisant of the consistently high number of Section 4 access requests being processed by the Garda Central Vetting Unit (GCVU) in Thurles (averaging 13,000 annually), the Office initiated an investigation in 2015 into compliance with Section 4(13) of the Acts from a criminal-records-check perspective. Forty organisations across a range of sectors were initially selected for closer examination in the form of a desk audit. A written questionnaire was issued that sought to identify companies engaged in the practice of requiring individuals to make subject access requests to An Garda Síochána. Based on the responses, a number of companies were selected for follow-up inspection.

While we are satisfied that no entity investigated sought to deliberately breach the provisions of the Data Protection Acts regarding enforced subject access requests, it is nevertheless the case that the investigation found that the actions of a number of organisations across the spectrum of recruitment, financial institutions and retail were in contravention of Section 4(13) of the Acts. These organisations were immediately instructed to cease. All of the organisations found to be in breach have formally written to this Office to say they have now ceased the practice. We will continue to combat any practices entailing enforced subject access requests and monitor organisations across a wide range of sectors throughout 2016.

PRIVACY AUDITS

In 2015, 51 audits and inspections were carried out by our audit team. Just under half of these were what are termed unscheduled inspections carried out under Section 24 of the Data Protection Acts, meaning that they arose from specific investigations or complaints and were additional to the planned programme or schedule of audits set out at the beginning of the year. Advance notice for these can vary from unannounced – two in 2015 – to a few weeks' notice. The aim of all of our audits and inspections is to check for compliance with the Data Protection Acts and to assist the data controller in ensuring that their data protection systems are as effective and comprehensive as possible. Audits are sometimes supplementary to investigations carried out by the Office 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.

Our annual audit programme is tailored to focus on a number of carefully selected sectors. In 2015, we concentrated on recruitment practices as part of a wider investigation into enforced subject access requests. Also selected for closer examination was the deployment of CCTV in a range of shopping centres and retail outlets and a comprehensive review of the data protection policies and procedures in three utility companies. In terms of the public sector, with the 2016 general election imminent, an audit was conducted of Dublin City Council's Franchise Section. The Road Transport Operator Licensing Unit (Department of Transport, Tourism and Sport) was also audited at the beginning of 2015.

In addition, a desk-based audit of 18 mobile apps was conducted as part of a Global Internet Privacy Sweep focusing on websites and apps either targeted at or popular among children.

Utility Companies

Three energy-supply utility companies were audited in 2015 and a key issue to emerge as a result of the audits was in relation to the deployment of third-party debt collectors. Issues were identified whereby letters issued seeking the payment of amounts outstanding did not clearly identify the data controller to whom the debt was owed. In all three audit reports, the Office issued a recommendation that the identity of the data controller must be clear to the data subject at all times in terms of letters issued by debt collectors operating on behalf of the data controllers.

We also recommended a review of call-handling procedures and caller-verification processes. This is an issue of priority for all organisations with large customer databases – to counter the dangers of private investigators or debt collectors obtaining information illicitly through 'blagging'.

In two cases, we also recommended that their systems need to be able to identify inappropriate access to personal data on their systems.

Retail Sector

The audit team continued with its programme of audits of shopping centres, with specific regard to CCTV cameras and the requirement for a CCTV policy to be in place. Based on audit findings, the Office met with retail representative bodies in order to highlight issues identified during the targeted programme of audits in shopping centres. Regarding initiatives being proposed by the retail sector to tackle shoplifting, the audit team referred to guidance published by the Office that sets out how sensitive personal data in relation to the commission, or alleged commission, of an offence may only be processed by a data controller (each retail outlet) itself for the purpose of pursuing legal action or where the processing is performed further to a specific statutory obligation. In the audit reports themselves, retailers were further advised that the sharing of any personal data by data controllers as to the commission or the alleged commission of an offence (different retailers sharing information/photos of individuals) would not be in compliance with the provisions of the Data Protection Acts.

A new area to emerge for consideration was the deployment of 'body-worn cameras' (BWCs) for security purposes in the retail environment. As a result of the series of audits of shopping centres, the audit team fed into the Office's new guidance on BWCs issued in December 2015. In line with our guidance on CCTV cameras, the use of any surveillance equipment must comply with the transparency requirements of data protection law.

Franchise Section, Dublin City Council

An audit was conducted of Dublin City Council's Franchise Section in order to examine procedures governing the compilation of the electoral register and the edited register.

Statistical analysis carried out over a number of years by the Office examined the numbers of individuals registering to vote each year and noted the consistent rise in growth of the edited register specifically in the Dublin City Council area (39%) as compared to the national rise, which was more modest (9.62%).

Register of Electors 2009 – 2015 National Figures

Year	Number of full register	Number on edited register	% on edited register
2009	3,234,155	267,117	8.26
2010	3,273,216	283,267	8.65
2011	3,280,899	290,410	8.85
2012	3,249,590	301,726	9.29
2013	3,265,880	303,407	9.29
2014	3,276,029	309,191	9.44
2015	3,317,927	319,081	9.62

Since 2004, registration authorities are required to publish two versions of the electoral register – the 'full' register and the 'edited' register. The full register lists everyone who is entitled to vote and can only be used for an electoral or other statutory purpose. The edited register contains the names and addresses of persons whose details can be used for a purpose other than an electoral or other statutory purpose, e.g. for direct-marketing use by a commercial or other organisation. When registering to vote, or amending their registration details if individuals do not opt out, they will automatically be included on the edited register and can therefore be legitimately marketed to.

The inspection of the Franchise Section in Dublin City Council in October 2015 found that there were 327,012 individuals on the DCC full electoral register and 128,367 individuals on the edited register – i.e. 39% of all individuals registered to vote in the Dublin City Council electoral areas were on the edited register.

No issues were found to be arising with regard to the operation of the Franchise Section in Dublin City Council. Overall, there was very high organisational awareness of data protection principles in evidence generally. This outcome was satisfactory, given the upcoming Dáil election, when electoral registers would be to the fore.

Insurance Sector and Penalty-point Data

One area selected for particular attention in 2015 was the data-processing activities of insurance companies regarding their access to penalty-point data, as provided for under Section 53(3)(c) of the Road Traffic Act 2010, which states:

'a vehicle insurer with the approval of the Minister may have access to and may inspect and examine endorsements on the entry relating to persons under this section and may take, or be supplied by the Minister with, such copies of entries or extracts from such entries as the vehicle insurer may reasonably require for the purposes of renewing approved policies of insurance, subject to such conditions as the Minister may determine.'

The purpose of the audits was to examine existing facilities within insurance companies to access penalty-point data in conjunction with the roll-out of a new facility, or sectoral 'hub' by Insurance Ireland, allowing for direct access to penalty-point data in real time via the Insurance Integrated Data Service hub. We will continue to examine this area further in 2016.

The audit found evidence of the retention of penalty-point data beyond 3 years (under the Road Traffic Act, penalty points remain on a licence record only for a period of 3 years) and, as a result, the Office is continuing to engage with the companies audited in 2016 to agree on an acceptable retention period and archiving solution.

Audit Findings

Themes identified in the 2015 audits include the following:

1. **Lack of data-retention policy**
   Under Section 2(1)(c)(iv) of the Act, 'data shall not be kept for longer than is necessary for that purpose or those purposes'. Nowadays, information can be kept cheaply and effectively on computer for a long time. This requirement places a responsibility on data controllers to be clear about the length of time for which data will be kept and the reason why the information is being retained. If there is no good reason for retaining personal information, then that information should be routinely deleted. Information should never be kept 'just in case' a use can be found for it in the future.

2. **Lack of signage of policy for CCTV systems**
   Unless CCTV systems are used with proper care and consideration, they can give rise to concern that the individual's 'private space' is being unreasonably invaded. Recognisable images captured by CCTV systems are personal data and are therefore subject to the provisions of the Data Protection Acts. A data controller needs to be able to justify the obtaining and use of personal data by means of a CCTV system. The presence of a CCTV system should also be properly indicated. Notification of CCTV usage can usually be achieved by placing easily read and well-lit signs in prominent positions.

3. **Excessive use of CCTV systems**
   CCTV should only be used for the purpose or purposes for which it is in operation: for example, security or health and safety. In general, it should not be used for other purposes: for example, staff monitoring.

4. **Lack of audit trails to identify inappropriate access**
   Only those required to access data for specific, previously delineated purposes should be in a position to do so. Organisations should maintain proper audit trails so as to guard against inappropriate access.

5. **Poor call-handling security procedures potentially allowing for 'blagging'**
   Where callers misrepresent themselves and trick employees of data-rich organisations, such as the Department of Social Protection or the HSE's Primary Care Reimbursement Service, into revealing data, that process is known as 'blagging'. The valuable data illegally obtained can then be illegally transferred. Organisations should ensure that they have robust call-handling procedures to guard against such practices.

6. **Illegal use of enforced subject access requests**
   Since 18 July 2014, it has been unlawful for employers to require employees or applicants for employment to make an access request seeking copies of personal data that is then made available to the employer or prospective employer.

   In cases where organisations are found to be non-compliant and subsequently refuse or fail to comply voluntarily, the Office may consider using the enforcement powers available to it.

7. **Lack of clarity in relation to data-controller/data-processor contracts**
   Contracts should be in place between a data controller and a data processor. The contracts should set out specific conditions on how personal data provided by the data controller to the data processor is to be processed, held securely and disposed of once the processing is finished.

8. **Clear identification of data controller where a debt collector has been engaged**
   At times, financial institutions engage debt-collection agencies to find a particular debtor. When this occurs, the agency gains access to a large amount of sensitive personal data. It is incumbent on organisations to clearly identify who the data controller is in such scenarios.

9. **Excessive use of biometric time and attendance systems**
   Biometric data may be created from physical or physiological characteristics of a person. These include a fingerprint, an iris, a retina, a face, the outline of a hand, an ear shape, a voice pattern, DNA and body odour. Biometric data might also be created from behavioural data such as hand-writing or keystroke analysis.

   An employer must conduct an assessment of the need for a biometric system and an evaluation of the alternatives before the introduction of any particular system.

10. **Excessive use of body-worn cameras**
    Our general guidance in this area is that we would consider that body-worn cameras should only be activated in extreme cases in response to specific pre-defined criteria, where it could be justified for security and safety purposes.

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

GUIDANCE

Key to the Office's engaged approach to regulation are the regular and meaningful consultations it undertakes with both public- and private-sector organisations. Rather than simply watching for transgressions, the Office has an engaged and proactive approach to regulation, meeting regularly with, for example, the large tech multinationals based in Ireland to discuss important features of EU data protection legislation. The team interacts with service providers at the inception of a product, service, policy or business initiative, allowing us the opportunity to assess compliance and seek the best result for the data subject. In 2015, the Office received 860 requests for specific guidance and assistance by public- and private-sector bodies and over 100 follow-up meetings took place.

We consulted on the following, not exhaustive, list of projects (exploratory or otherwise) during 2015:

- Credit Reporting Act 2013
- Common Reporting Standards CRS as drafted by OECD
- The Health Identifier
- Education – Primary Online Database (POD)
- Eircode
- Department of Expenditure and Reform – Data Sharing Bill
- Department of Expenditure and Reform – Central Collection Agency
- Road Safety Authority – Identification of Disqualified Drivers
- Department of Children and Youth Affairs – Reform of the Guardian ad Litem Service
- Department of Defence – 1916 Commemorations

- Department of Defence/Office of Emergency Planning (OEP) – Flood Action Plan
- Joint Agency Approach – Monitoring of Employment in the Fisheries Sector
- HSE – Under-Sixes and Free GP Care
- Genetic Data and Sequencing Health Research
- Local Authorities and Housing Lists
- Health Research Board and Proposals for Enabling Health Research in Ireland
- Adoption Authority and the Information and Tracing Bill 2015
- Mount Carmel Hospital Group Liquidation
- Consultation by a variety of stakeholders with the Office on the legal basis necessary to underpin the potential establishment of a national anti-fraud database for the banking sector
- Consultations by a broad range of organisations with the Office seeking guidance on EU to USA personal data transfer mechanisms post the striking down of Safe Harbour.

In 2015, the Office updated its detailed guidance on three major data protection issues: drones, CCTV and body-worn cameras.

Drones

These small aircraft operate without a human pilot. Long deployed for military use, they have, in recent years, been embraced by civilians for private use. Because of this, it was necessary for this Office to issue comprehensive and timely guidance on the potential data-privacy impacts that improper use of this technology might have.

CCTV

We have also seen a marked expansion in the use and sophistication of CCTV systems, which are now, in some cases, advanced enough to recognise faces and record both images and sounds, an added layer of monitoring.

Additionally, following the CJEU ruling in the Ryneš case on 11 December 2014, it has been clarified that the domestic-use exemption for CCTV cameras contained in Article 3(2) of the Data Protection Directive 95/46/EC for 'personal or household activity' does not allow for the recording by domestic CCTV cameras of space beyond the boundaries of one's own property and capturing the activities of other members of the public going about their daily business.

Such systems must be used with proper care and consideration as they can give rise to concern that the individual's private space is being unreasonably invaded. A data controller needs to be able to justify the obtaining and use of personal data by means of a CCTV system and have a proper written CCTV policy in place outlining the position regarding requests for access to footage by third parties such as An Garda Síochána.

Body-worn Cameras

In line with our guidance on CCTV cameras, the use of any surveillance equipment must comply with the transparency requirements of data protection law. Particular issues arise with regard to body-worn cameras or other mobile image-recording devices, which may lead to inadvertent recordings. Additionally, body-worn cameras often have voice-recording capability, which the Office considers to be an added intrusion into the privacy and data protection rights of individuals. Section 2(1)(c)(iii) of the Acts require that data are 'adequate, relevant and not excessive' for the purpose for which they are collected. This means that the data from such processing should be limited to what is strictly necessary to achieve a specific purpose, and so the Office would expect that a data controller would have carried out detailed risk and privacy impact assessments prior to roll-out.

Guidance in Future

For 2016, we have renewed our commitment to completely redeveloping our website by providing comprehensive, easily accessible and clear guidance. This will include the generation of guidance in Irish for publication on the Irish language version of our website – www.cosantasonrai.ie. We have engaged a dedicated legal resource to assist us in delivering this objective and look forward to the outcome of this important project.

BINDING CORPORATE RULES

Binding Corporate Rules (BCRs) are internal rules adopted by multinational groups of companies. This is an alternative to the company having to sign standard contractual clauses each time it needs to transfer data to a member of its corporate group. These rules define the global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries that do not provide an adequate level of protection. Essentially, BCRs act as a safeguard for such transfers and ensure that all transfers made within a company group benefit from an adequate level of protection.

BCRs must be approved under the EU cooperation procedure and in some cases companies must seek further authorisation of transfers from national data protection authorities. In this jurisdiction, such national approval is not required as we are members of the mutual recognition procedure and therefore respect the decision of the lead DPA. It should be noted that the BCRs do not provide a basis for transfers made outside of the company group.

BCRs were a creation of the Article 29 Working Party but, going forward, Article 47 of the GDPR will give legal recognition to the process and this will probably result in an increase in applications once the GDPR is in place.

In 2015, the Office was acting as the lead reviewer in four BCR applications. Details of companies currently undergoing the approval procedure cannot be released until the BCR has been approved. We also assisted the Belgian DPA with their assessment of the Starwood Hotels and Resorts' BCR application, which has since been approved. The BCR reviews are ongoing along with the additional BCR applications received in the early part of 2016.

TYPICAL ENGAGEMENT WITH TECH MULTI-NATIONALS

In 2015, we saw our already continuous engagement with multinational organisations in Ireland amplified. Controllers have sought, among other things, our advice and guidance on a wide variety of organisational and technology matters. Examples of such engagement are set out below. In addition, this Office established a forensics technical laboratory. We have invested in equipment for the purposes of developing our technical capabilities to assist in performing technical audits, technical investigations and technical research. This forensics technical laboratory has been set up on an isolated independent network, allowing the replication and testing of different scenarios using various software tools and technical equipment. It has improved the ability of the Office, in the course of ongoing work, to perform technical analysis on different software versions and allowed tests to be repeated by different technologists using the same starting criteria to validate results. It also allowed testing of this software across multiple devices, e.g. laptops and mobile devices, and various operating systems, and enabled us to check whether the behaviour was consistent across these varying environments.

The follow are examples of engagement with a number of the tech multinational companies during 2015:

- Completion of a progress review of LinkedIn's implementations of our audit recommendations of the 2013/14 audit. This involved correspondence, meetings and reviews of the service and supporting documentation and data, followed by a comprehensive report on the state of the LinkedIn service as we found it. We continued to engage and pursue matters throughout 2015.

- Meetings and correspondence with Facebook Ireland Ltd after the launch of their revised Data Policy and Cookie Statements, privacy settings and controls. This included organisational and technical review of settings and controls in relation to advertising, updated and new features such as legacy accounts and family tagging, handling of consent to the use of cookies, personal data inventories, use and retention of location data, use of contact data, and an extensive engagement on details of access request handling.

- Updates from Microsoft in respect of their European establishments and businesses and a technology review of the newly released and updated privacy policy.

- Many meetings and much correspondence in relation to transfer rules based on contractual clauses and binding corporate rules from data processors and controllers established here and in Europe.

- Commencement of a focused technology-based audit of certain areas of Adobe Systems Ireland's establishment and products.

- Meetings and correspondence with AirBnb in respect of their new establishment in Ireland and the operation of their service and product offering in Europe.

- Several meetings with organisations who are exploring the possibility of establishing here as either a data controller or processor in the financial-services industry, 'Big Data' and analytical processing.

- Meeting and correspondence with Google regarding the implementation of the CJEU 'Right to be Forgotten' judgment.

Engagement with LinkedIn

We met with the senior LinkedIn policy and data protection representatives in Dublin on numerous occasions to receive updates on recommendations made on foot of the 2013 audit, and to provide guidance and best-practice recommendations concerning LinkedIn products and features. These meetings centred around many items, a selection of which are referred to below. Over the course of 2015, there have been face-to-face meetings, video conferences, email exchanges and telephone calls with LinkedIn personnel on various data protection and ePrivacy issues related to the current LinkedIn service and proposed changes and new features.

This engagement occurred in parallel to exchanges with LinkedIn on day-to-day matters as well as queries that our Office received from the public. In 2015, we saw some constructive engagement and discussions about new product features, updates to existing products, and briefings on companies that were acquired by LinkedIn. In a number of cases, this resulted in alterations to the substance or schedule of such planned changes. This engagement with LinkedIn continues in 2016 as it continues to revise and develop new products and features. Some of the alterations made by LinkedIn on foot of our 2013 audit are described below.

Member Settings

During the audit of 2013, we highlighted to LinkedIn the importance of relevant in-context and in-product settings that improve the control members have over their data and make it easier for members to access and use these controls. This is an important element that information-society services must pay attention to in order to support their efforts in transparency and to ensure the quality and validity of the consent they obtain from their users. To that end, in pursuit of our guidance, LinkedIn has:

- adjusted the layout and location of in-product settings on a member's profile;
- updated the accessibility of settings in some of LinkedIn's mobile apps;
- added inline settings that allow members to choose audiences for their shared content.

Further, we have emphasised the significance of how LinkedIn settings are presented to data subjects and we note that LinkedIn have made efforts to redesign settings in order to simplify the control process for data subjects.

Data-access Requests

We also engaged with LinkedIn in relation to the Data Access Request tool that was created as a result of our recommendations arising from LinkedIn's obligations under Section 4 of the Data Protection Act 2008. During 2015, this engagement centred around the consistency of LinkedIn's responses to Section 4 Subject Access Requests through to the new tool and via other communications channels. While the tool is not meant to be a replacement for an official response to a Subject Access Request, it is a convenient method for users to exercise this right when requesting certain personal data held by LinkedIn about them. In 2015, we noted that the development of this tool should include connection information and email messaging. We continue to encourage LinkedIn to augment the data types available to users of this tool in support of their Section 4 obligations.

Management of Cookies

A comprehensive cookie-management framework was recommended to LinkedIn as a means to assist them in meeting the requirements on data controllers from an ePrivacy perspective (see SI 336 of 2011). The intention of such a framework is to support LinkedIn's design and engineering teams in the consistent use of cookies or other browser and device storage. It also should aim to provide transparency and clarity to data subjects about the collection, use and retention of LinkedIn data held on a user's equipment, both on and off the LinkedIn service. We also emphasised that LinkedIn should address their obligations with regard to prominent notification and information in their cookie policy. We asked that LinkedIn provide more detail in its cookie policy relating to concepts such as Do Not Track, opt-out controls, third-party cookies, non-cookie storage mechanisms and categorisation of individual cookies. LinkedIn has now set up a 'Cookie Council' to consistently address and manage cookie-related matters across their service offerings and processing operations, and the work on these matters is ongoing. We note that our recommendations are being addressed and work is in progress. We continue to monitor and engage with LinkedIn on the efficacy, consistency and suitability of the roll-out of these changes made in 2015 and upcoming in 2016.

Privacy by Design

Throughout 2015, we highlighted the importance of privacy by design for all data controllers with complex product offerings, those with large and multinational audiences, and often where technology is a key element in product delivery. For organisations, this is a key concept that directly benefits data subjects. It assists those organisations in meeting their data protection obligations from business case and design through to product maintenance and end-of-life. It aims to ensure that all those within the organisation who are involved, engaged or related to an organisation's products or services actively consider and address data protection from concept to delivery and on to after-care. We specifically asked LinkedIn to further develop the close relationship between its legal and engineering teams to ensure that privacy continues to be considered during all phases of product design. To that end, LinkedIn last year established a centralised team of privacy and security engineers in Dublin to test and train engineering and product personnel. This team is closely tied with LinkedIn's legal team in Ireland, and together they work to encourage the use of privacy by design methodologies throughout the LinkedIn organisation. Again, we will continue to monitor and gauge the effectiveness and application of this new team in 2016.
Beyond the items mentioned above, we continue in 2016 to work with LinkedIn on changes addressing audit recommendations in both the technology and organisation, and on new and updated features, apps and services offered by LinkedIn and its partners or affiliates, both on and off the LinkedIn platform.

Engagement with Facebook

During 2015, staff of this office engaged with senior management of Facebook in relation to a wide variety of data protection issues. This Office reviewed various new policies and products and provided guidance and best-practice recommendations on issues. Outlined below are some examples of issues considered by this Office. This engagement will continue in 2016.

Online Behavioural Advertising Opt-out

Members of the public are becoming increasingly aware of the tracking of their online behaviour. In line with current, applicable data protection legislation, it is important that all users be able to exercise more choice as to how and for what purpose their data is processed.

Online Behavioural Advertising (OBA) is a means of using information about a user's web-browsing activity so as to categorise groups of users into interest groups and enable advertisements to be directed to

the users based on their interests. In many cases, the information used for targeting adverts is not personal in that the user cannot be identified. Where personally identifiable advertising is used, the privacy policy and notification to users must provide clear understandable and comprehensive information in relation to same so that the user can make an informed decision regarding the use of their data, distinguish between interest-based advertising and advertising that is customised to him/her, and exercise a choice to opt out as required.

On 15 September 2015, following intense engagement with the Office over a number of months regarding the roll-out of online behavioural advertising in the EU, Facebook Ireland Ltd announced the introduction of additional functionality that allows users to opt out of online behavioural advertising through the Facebook service itself, meaning that once a user opts out using this tool, Facebook will apply the choices that have been made everywhere they use Facebook. In other words, the choices users make apply across devices. This tool was adopted in response to feedback from us and other stakeholders that it would be preferable for users to exercise their OBA preference across the internet without having to go to a third-party site that used cookies.

Privacy Basics

Throughout its engagement with Facebook Ireland Ltd, the Office maintains that when users seek information about privacy controls on the medium, there should be means to disseminate that information in addition to the Data Policy. In response to our feedback, Facebook Ireland Ltd developed and launched Privacy Basics, which provides users with an animated learning tool and interactive how-to guides that allow users to control the use of their information across a wide variety of topics.

Privacy Check-up

The Office, in all its interactions with Facebook Ireland Ltd, continually stresses the importance of users understanding who can see the content that is shared. In response to this feedback, Facebook Ireland Ltd developed and launched its Privacy Check-up tool.

Privacy Check-up is a privacy-enhancing tool that assists Facebook users to review and adjust their privacy settings, helping users make sure that they are sharing content appropriately and centralising users' privacy choices.

Download Your Information

In response to recommendations contained in the Office's audit, Facebook Ireland Ltd has developed a tool that allows users to easily download a copy of their Facebook data ('Download your information' or 'DYI'). Facebook Ireland Ltd now also provides a dedicated contact point by way of email address – datarequests@support.facebook.com – for users who have detailed requirements for access to personal-data types or complaints about the availability of some data.

GLOBAL PRIVACY SWEEP – WEBSITES AND MOBILE APPLICATIONS

In June 2007, OECD governments adopted a Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy. The recommendation called for member countries to foster the establishment of an informal network of Privacy Enforcement Authorities to support joint enforcement initiatives and awareness campaigns. A Global Privacy Enforcement Network (GPEN) was established in 2010 on foot of this recommendation. Its aim is to create cooperation between data protection regulators worldwide in order to strengthen personal privacy, and it is currently made up of 51 data protection authorities across 39 jurisdictions.

Between 11 and 15 May 2015, 29 data protection regulators around the world, including Ireland, participated in the third GPEN Sweep, which examined the data-privacy practices of 1,494 websites and mobile applications (apps) aimed at or popular among children.

The international results found that 41% of websites and apps assessed raised concerns, particularly around the amount of personal data collected and the manner in which it was subsequently shared with third parties.

The international results concluded that:

- Of the sites/apps examined, 67% collected children's personal information.
- Only 31% of sites/apps had effective controls in place to limit the collection of personal information from children. Particularly concerning was that many organisations whose sites/apps were clearly popular with children simply claimed in their privacy notices that they were not intended for children, and then implemented no further controls to protect against the collection of personal data from the children who would inevitably access the app or site.
- Half of sites/apps shared personal information with third parties.
- 22% of sites/apps provided an opportunity for children to give their phone number and 23% allowed them to provide photos or video. The potential sensitivity of this data is clearly a concern.
- 58% of sites/apps offered children the opportunity to be redirected to a different website.
- Only 24% of sites/apps encouraged parental involvement.

- 71% of sites/apps did not offer an accessible means for deleting account information.

In Ireland's case, the sweep involved the examination of 18 apps and websites (both international and Irish) that are popular with Irish children. The Irish results found that the sites/apps tested requested technical data such as cookies (61%), IP address (28%), UID (50%) and geo location (28%). The sweep team also noted that 45% of sites/apps tested carried third-party advertising, much of which would not be relevant to or appropriate for children.

The overall sweep findings did identify some areas of good practice, with certain websites and apps providing effective protective controls, such as parental dashboards, and pre-set avatars and/or usernames to prevent children inadvertently sharing their own personal information. Other good examples included chat functions that only allowed children to choose words and phrases from pre-approved lists, and use of just-in-time warnings to deter children from unnecessarily entering personal information.

However, websites and apps targeted at or popular with children need to greatly improve data security.

The Irish sweep identified 5 sites/apps that raised particular concerns for this Office. Although 4 of these were not based in this jurisdiction, we carried out further more detailed analysis of each these sites/apps. In one case, we alerted the ICO in the UK of our findings. In another, we contacted the ISAI regarding inappropriate advertising being carried on an Irish website. Further follow-up was not warranted or possible with the remaining sites/apps, as one has resolved the issues, another no longer exists, and in the third case we have been unable to identify the relevant jurisdiction.

EUROPEAN UNION

New EU Data protection Laws

The European Commission proposals for a new General Data Protection framework, which were published in 2012, continued to be the subject of much discussion in 2015. In December 2015, a political agreement was reached with the European Commission, Parliament and the Council following 'trilogue' negotiations between the three institutions. The reform consists of two instruments: the General Data Protection Regulation and the Data Protection Directive in relation to personal data processed for law-enforcement purposes. The GDPR will enable people to better control their personal data and will allow businesses to make the most of the opportunities of the Digital Single Market. The DPD for the police and criminal-justice sector will ensure that the data of victims, witnesses and suspects of crimes are duly protected in the context of a criminal investigation or a law-enforcement action. These harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The reform will harmonise and modernise data protection laws in Europe. According to a Eurobarometer survey, two-thirds of Europeans (67%) stated they are concerned about not having complete control over the information they provide online. The data protection reform will strengthen the right to data protection, which is a fundamental right in the EU, and allow citizens to have trust when they share their personal data.

Article 29 Working Party

In 2015, the Commissioner or the Deputy Commissioner 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. During 2015, it exchanged ideas on many operational and policy issues. In October 2015, Article 29 held its first emergency plenary meeting to examine the consequences of the Schrems CJEU ruling of that month. At that meeting, Article 29 clarified that transfers under Safe Harbour were now unlawful and undertook to examine the consequences of the ruling on the alternative mechanisms of transfer (SCCs and BCRs) and urged member states and the Commission to find the necessary political and legal solutions to EU–US data transfers.

Article 29 Subgroups

During 2015, members of staff attended meetings of the Article 29 subgroups. Our participation in the Article 29 Technology Subgroup is key to our commitment to consistency in policy and enforcement at a European level for technology issues. The topics covered in these meetings are wide and varied but have resulted this past year in cooperation on opinions regarding matters such as the use of drones, cloud computing and a cookie sweep across Europe. Over the course of 2015, the Google and Facebook privacy policies remained in focus for the Technology Subgroup and continue so in 2016.

Other subgroups have been active in the areas of contract model clauses, binding corporate rules, national security, legitimate interests, applicable law and risk approaches to data protection. Ireland's active role in these groups and the drafting of opinions means that we can share expertise and knowledge with colleagues in Europe on a broad range of topics, while also discussing approaches to enforcement, and understanding the differences that sometimes occur in national implementations of the EU Data Protection Directive.

Joint Supervisory Bodies

During 2015, members of staff attended meetings of the joint supervisory bodies of JSB Europol and JSA Customs. These groups were established to monitor the processing of personal data in large pan-European databases operated by Europol and European customs authorities.

Data Breaches

The Office also participated in a large-scale pan-European Data-Breach Exercise in November 2015 in which members of staff experienced first-hand the methodology of dealing with a data breach that transcends borders and affects data subjects in a number of EU member states.

The Court of Justice of the European Union (CJEU) Maximilian Schrems and Facebook (Case C-362/14)

The hearing at the CJEU into Mr. Schrems' complaint against the Irish DPC was heard in Luxembourg in March 2015. The Advocate General issued his opinion in this regard on 23 September 2015. Shortly thereafter on 6 October, the CJEU issued its important and far-reaching ruling in the case, which included the striking-down of Safe Harbour.

In the subsequent hearing in the Irish High Court on 20 October 2015, the matter was remitted for consideration to the DPC, which undertook to investigate '... the substance of the complaint with all due diligence'.

The Court invited Mr. Schrems to submit a reformulated complaint in light of the striking-down of Safe Harbour and this is the subject of ongoing investigation.

The CJEU issued two other data protection-specific judgments during 2015:

- In October 2015, the CJEU issued a ruling in the Smaranda Bara case (C-201/14), which involved the sharing of data between the tax authorities and the National Health Insurance Fund in Romania for the purposes of collecting any applicable arrears. The Court in that case held that EU law precludes the transfer and processing of personal data between two public administrative bodies without the persons concerned (data subjects) having been informed in advance. This case provided important clarifications for public bodies that may wish to engage in data-sharing.
- In the same month, in Case C-230/14 Weltimmo v Nemzeti, the Court studied the issue of jurisdiction and 'establishment' for the purposes of the Data Protection Directive (95/46/EC) in a scenario that concerned a Slovakian registered company but which advertised Hungarian properties in Hungarian language and charged advertising fees directed to a Hungarian bank account. The full judgment of the Court needs to be studied on its specific facts but, regardless, the GDPR will resolve many of the issues this case examined in relation to both jurisdictions of DPAs and establishment of controllers.

OTHER INTERNATIONAL ACTIVITIES

The Office was represented at the Global Privacy Enforcement Network (GPEN) signing ceremony and associated meetings themed '2016 and beyond – A New Era in Global Enforcement Cooperation'. GPEN is an informal network of Privacy Enforcement Authorities supporting joint enforcement initiatives and awareness campaigns worldwide and is made up of 51 data protection authorities across 39 jurisdictions, including this Office.

We continued to foster trans-Atlantic relations by attending events organised by the US Chamber of Commerce and the Federal Trade Commission.

Beyond the EU level, we actively continue to engage in technology-related matters in the International Working Group on Data Protection in Telecommunications (IWGDPT), in the newly formed Internet Privacy Engineering Network (IPEN) and we participated in the 37th International Conference of Data Protection and Privacy Commissioners in Amsterdam.

APPENDICES

List of Organisations Audited or Inspected in 2015

Case Studies
1) Marketing offences by MTS Property Management Limited – prosecution
2) Marketing offences by Greyhound Household – prosecution
3) Marketing offences by Imagine Telecommunications Business Limited – prosecution
4) Marketing Offences by Eircom Limited – prosecution
5) Defence Forces Ireland – failure to keep data safe and secure
6) Further processing of personal data by a state body
7) Supermarket's excessive use of CCTV to monitor member of staff
8) Disclosure of personal information to a third party by the Department of Social Protection
9) Covert CCTV installed without management knowledge
10) Danske Bank erroneously shares account information with third parties
11) Failure to update customer's address compromises the confidentiality of personal data
12) Unfair use of CCTV data

Presentations and Engagements with Stakeholders
Registrations Statistics
Account of Income and Expenditure
Energy Report

LIST OF ORGANISATIONS AUDITED OR INSPECTED IN 2015

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.

- Grafton Recruitment
- Electric Ireland
- Dublin Bike Scheme
- Road Transport Operator Licensing Unit
- Marks & Spencer
- Woodies DIY
- SSE Airtricity
- Aldi
- Croskerrys Solicitors
- Rigney Dolphin
- Littlewoods
- Dalmac Recruitment & Aviation Services
- Bord Gáis
- Pepper Ireland
- MJG Investigations
- ECO Group Services
- James Cowley & Associates
- Dublin City Council Franchise Section
- Shoreline
- Oracle
- Allied Irish Bank (two separate audits were conducted regarding discrete matters)
- Ulster Bank
- Start Mortgages
- Aviva Insurance
- Axa Insurance
- National Recruitment Federation (desk audit)
- Adobe
- Kerry Foods
- Arizun Services
- Irish Auditing & Accounting Supervisory Authority
- Secondary Education Committee
- Mater Misercordiae University Hospital
- Swords Health Centre
- Midlands Regional Hospital
- Aer Lingus
- BDO Chartered Accountants
- Irish Bank Resolution Corporation
- Dunnes Stores
- Bank of Ireland
- Barberstown Castle
- CEIST Ltd
- Lawlor Partners, Solicitors
- J.F. Harrington & Company
- Allianz
- State Claims Agency
- Zurich Insurance
- Greendoor Property Management
- QED Recruitment
- Europol
- Workplace Relations (Equality Tribunal)

CASE STUDIES

Case Study 1:
Marketing offences by MTS Property Management Limited – prosecution

We received a complaint in February 2013 from an individual who received marketing SMS messages from MTS Property Management Limited advertising the company's property-management services. The complainant informed us that she had dealt with the company on one occasion over five years previously but she did not consent to her mobile phone number being used for marketing purposes. She also pointed out that the SMS messages that she received did not provide her with a means of opting out.

Our investigation of this complaint became protracted as the company denied knowledge of the mobile number to which the SMS messages were sent and it denied knowledge of the account holder of the sending phone number. However, our investigation established sufficient evidence to satisfy itself that MTS Property Management Limited was responsible for the sending of the marketing SMS messages to the complainant. We decided to prosecute the offences.

MTS Property Management Limited had come to our attention previously in the summer of 2010 when two individuals complained about unsolicited marketing SMS messages sent to them without consent and without the inclusion of an opt-out mechanism. Following the investigation of those complaints, we warned the company that it would likely face prosecution if it committed further offences under Regulation 13 of SI 336 of 2011 at any future time.

At Dublin Metropolitan District Court on 23 February 2015, MTS Property Management Limited pleaded guilty to one charge of sending an unsolicited marketing SMS without consent and it pleaded guilty to one charge of failing to include an opt-out mechanism in the marketing SMS. The Court convicted the company on both charges and it imposed two fines of €1,000 each. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

Case Study 2:
Marketing offences by Greyhound Household – prosecution

In May 2014, we received a complaint against Greyhound Household from an individual who received an unsolicited marketing phone call on his mobile telephone from the company's sales department. The same individual had previously complained to us in December 2013 as he was receiving marketing SMS messages from Greyhound Household that he had not consented to receiving. He informed us that he had ceased being a customer of the company in May 2013. Arising from the investigation of the previous complaint, Greyhound Household had undertaken to delete the former customer's details and it apologised in writing to him. On that basis, we concluded the matter with a formal warning to the effect that any future offences would likely be prosecuted.

On receipt of the latest complaint, we commenced a further investigation. Greyhound Household admitted that a telephone call was made to the complainant's mobile phone number without consent but it was unable to explain why his details had not been deleted in line with the company's previous undertaking. We decided to prosecute the offence.

At Dublin Metropolitan District Court on 23 February 2015, Greyhound Household pleaded guilty to one charge of making an unsolicited marketing phone call to a mobile phone number without consent. The Court applied Section 1(1) of the Probation of Offenders Act subject to the defendant making a charitable donation of €1,000 to Pieta House. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

Case Study 3:
Marketing offences by Imagine Telecommunications Business Limited – prosecution

In March 2015, we received a complaint against Imagine Telecommunications Business Limited from a company that had received unsolicited marketing telephone calls. The same company had previously complained to us in 2014 about repeated cold calling to its offices. Despite having submitted an opt-out request to Imagine Telecommunications Business Limited, it continued to receive marketing phone calls. Following our investigation of the first complaint, and having been assured that the phone number of the complainant company had been removed from the marketing database, we issued a formal warning to Imagine Telecommunications Business Limited that any future offences would likely be prosecuted.

On investigating the current complaint, we were informed by Imagine Telecommunications Business Limited that it had failed to mark the telephone number concerned as 'do not contact' on the second of two lists on which it had appeared. This led to the number being called again in March and June 2015. It stated that the only reason the number was called after the previous warning was due to this error and it said that it took full responsibility for it.

We prosecuted the offences at Dublin Metropolitan District Court on 2 November 2015. Imagine Telecommunications Business Limited pleaded guilty to one charge of making an unsolicited marketing telephone call without consent. The Court applied Section 1(1) of the Probation of Offenders Act conditional upon a charitable donation of €2,500 being made to the Merchant's Quay Project. Prosecution costs were recovered from the defendant.

Case Study 4:
Marketing offences by Eircom Limited – prosecution

We received complaints from two individuals in February and April 2015 concerning marketing telephone calls that they had received on their landline telephones from Eircom Limited. In both cases, and prior to lodging their complaints, the individuals had submitted emails to Eircom Limited requesting that they not be called again. Eircom's Customer Care Administration Team replied to each request and informed the individuals that their telephone numbers had been removed from Eircom's marketing database. Despite this, each individual subsequently received a further marketing telephone call in the following months, thus prompting their complaints to this Office.

Eircom informed our investigations that the agents in its Customer Care Administration Team who handled the opt-out requests had not updated the system to record the new marketing preference after sending out the replying email to the individuals concerned. It undertook to provide the necessary refresher training to the agents concerned.

Separately, a former customer of Eircom complained in May 2013 that he continued to regularly receive unsolicited marketing phone calls from Eircom on his landline telephone despite clearly stating to each caller that he did not wish to receive further calls. He stated that the calls were numerous and that they represented an unwarranted intrusion into his privacy. Eircom continued to make a further ten marketing telephone calls to the individual after the commencement of our investigation of this complaint. Our investigation subsequently established that this former customer had received over 50 marketing contacts from Eircom since 2009 when he ceased to be an Eircom customer. Eircom explained that the continued calls arose from a misunderstanding of what systems the former customer's telephone number was to be opted out from.

In October 2014, an Eircom customer complained that he had received a marketing SMS from Eircom that did not provide him with a means to opt out of receiving further marketing SMS messages. Eircom informed our investigation of this complaint that the inclusion of an opt-out is the norm in all of its electronic-marketing campaigns but, in this instance, and due to human error, the link to the necessary opt-out had not been set properly. Our investigation established that this error affected over 11,600 marketing messages that were sent in the campaign concerned.

We proceeded to prosecute the offences identified on foot of the complaints received in the aforementioned cases. At Dublin Metropolitan District Court on 2 November 2015, Eircom Limited pleaded guilty to six charges of making unsolicited marketing calls without consent and it pleaded guilty to one charge of sending a marketing SMS without a valid address to which the recipient may send an opt-out request. The Court applied Section 1(1) of the Probation of Offenders Act conditional on the defendant making donations amounting to €35,000 as follows: €15,000 to Pieta House, €10,000 to LauraLynn (Children's Hospice) and €10,000 to Our Lady's Children's Hospital, Crumlin. The company agreed to pay the prosecution costs incurred by this Office.

Case Study 5:
Defence Forces Ireland – failure to keep data safe and secure

A member of the Defence Forces made a complaint to this Office that certain personal data relating to him was not kept safe and secure by the Defence Forces.

The circumstances of the individual's complaint to our Office arose when a Military Investigating Officer (MIO) was appointed to review an internal complaint made by him as a member of the Defence Forces. Subsequently, the Defence Forces Ombudsman was appointed to review the process of the handling of the complaint and, during the course of its review, it was ascertained that the MIO could not supply details of interview notes of an interview he had conducted with the complainant as he had stored them at an unsecure location and they were damaged or lost following flooding and a burglary at that location when the MIO was on an overseas mission. The unsecure location was in fact the MIO's private house

We raised the matter with the Defence Forces, who confirmed the complainant's allegation that the notes had been stored at an unsecure location and had been damaged or lost as stated.

The Defence Forces informed us of the measures taken to keep data safe and secure, and referred us to its Administration Instruction, which provides for the prohibition of removal of records.

The Defence Forces further stated that the removal of records from their place of custody to a private residence would breach this instruction and that a breach of this provision may constitute an offence under S.168 of the Defence Act 1954. It advised that, as the MIO was no longer a serving member of the Defence Forces, he is not subject to military law.

The Defence Forces unequivocally acknowledged that the loss of the data in this case should not have occurred and was fully regretted. It informed us that it had recently undertaken a full review of practices and procedures in respect of both the processing and disclosure of data to mitigate the possibility of any future unauthorised or accidental disclosure of personal data.

The Commissioner's decision on this complaint issued in June 2015, and it found that the Defence Forces contravened Section 2(1)(d) of the Data Protection Acts by failing to take appropriate security measures against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the complainant's personal data when it allowed it to be stored at an unsecure location, namely a private house.

This Office acknowledges that the Defence Forces has procedures in place in relation to the protection of personal data as set out in its Administration Instruction. However, those procedures were not followed in this case and when an official record was removed from its place of custody, it resulted in the complainant's personal data being lost or stolen because the appropriate security measures in place were not followed.

There are many workplace scenarios where staff and managers, in particular, may need to take files, including personal data, home with them. Extreme caution should always be exercised in such cases to ensure that there is no risk to the security of personal data either in the transit of the files or while the files are in the employee's home. Data controllers must ensure that employees act in a responsible manner with regard to the safe custody and handling of workplace files. This demands a proper system that records the taking of and returning of files and the following of prescribed procedures for the safe keeping of personal data while the files concerned are absent from the workplace. Likewise, it is critical that employees are prohibited from emailing official files from their workplace email account to their personal email account for afterhours work or for any other reason. In such situations, data controllers lose control of personal data that they are obliged by law to protect.

Case Study 6:
Further processing of personal data by a state body

In February 2015, we received a complaint from an employee of a state body in relation to the alleged unfair processing of his personal data. The complainant stated that, in the course of a meeting, he had been advised that his manager had requested access to data from his security swipe card in order to compare it with his manually completed time sheets. The complainant explained that this had been carried out without any prior consultation with him or his line manager. By way of background, the complainant informed us that the security swipe cards used by the employees are for accessing the building and secured areas only, and are not used as a time management/attendance system.

We sought an explanation from the body concerned as to how it considered that it had complied with its obligations under the Data Protection Acts in the processing of the complainant's personal information obtained from his swipe-card data. We also advised it that we had sight of the relevant section of its staff handbook and we noted that there was no reference to the swipe card being used for the purpose of checking attendance.

We received a response explaining that the swipe-card data relating to the complainant was handed over to the complainant's manager in good faith on the basis that it was corporate rather than personal data. The organisation also confirmed that it checked the staff handbook and any other information that may have been circulated to staff regarding the purposes of the swipe card and that there was no mention of the use of swipe cards in relation to recording time or attendance. It advised that the focus of the information circulated with regard to swipe cards was on security and access only.

After consideration of the response received, along with the content of the complaint, we informed the organisation concerned that we considered that the Data Protection Acts were breached when the employee's swipe-card details were provided to his manager to verify his working hours. We referred to the provisions of Section 2(1)(c)(ii) of the Data Protection Acts, which state that data shall not be further processed in a manner incompatible with the purpose for which it was obtained. Given that we considered the information concerned had been processed in contravention of the Data Protection Acts 1988 and 2003, we required an assurance that all email records created in relation to the further processing of the swipe-card details concerned be deleted from its systems; this assurance was duly provided.

The complainant in this case agreed, as an amicable resolution to his complaint, that he would accept a written apology from his employer. This apology acknowledged that the complainant's data protection rights had been breached and it confirmed that the organisation had taken steps to ensure that this type of error did not recur in the future.

This case highlights the temptation organisations face to use personal data that is at their disposal for a purpose other than that for which it was originally obtained and processed. The scenario outlined above is not uncommon, unfortunately. Time and attendance monitoring may occasionally prove difficult for managers, and contentious issues arise from time to time. The resolution of those issues should not involve an infringement of the data protection rights of employees similar or otherwise to the circumstances in this case.

Case Study 7:
Supermarket's excessive use of CCTV to monitor member of staff

A former staff member of a supermarket submitted a complaint to this Office regarding her employer's use of CCTV.

The complainant informed us that she had been dismissed by her employer for placing a paper bag over a CCTV camera in the staff canteen. She informed us that the reason for her covering the CCTV camera was that when she was on an official break in the staff canteen, a colleague styled her hair. The complainant also stated that the camera was placed in the corner of the staff canteen and there was no signage to inform staff that surveillance was taking place. She informed us that she was never officially advised of the existence of the camera nor had her employer ever informed her of the purpose of the CCTV in the canteen.

In its response to our investigation, the supermarket informed us that the complainant was dismissed for gross misconduct, which occurred when she placed the bag over the camera in the canteen to prevent her actions being recorded and thereby breaching the store's honesty policy as outlined in the company handbook. The supermarket owner informed us that the operation of CCTV

cameras within the retail environment was to prevent shrinkage, which can arise from customer theft, waste and staff theft. He stated that it was also used for health and safety, to counter bullying and harassment and for the overall hygiene of the canteen. In relation to the incident concerning the complainant, the owner informed us that, on the day in question, the store manager noticed some customers acting suspiciously around the off-licence area and that on the following day CCTV footage was reviewed. It was during the viewing of the footage in relation to suspicious activity in the off-licence area that he noticed the complainant putting a bag over the camera.

Following an inspection by one of our Authorised Officers, we informed the supermarket owner that, in our view, there was no justification from a security perspective for having a camera installed in the canteen area.

The complainant in this case declined an offer of an amicable resolution and she requested a formal decision of the Commissioner.

The decision by the Commissioner in January 2015 found that the supermarket contravened Section 2(1)(c)(iii) of the Data Protection Acts, 1988 and 2003, by the excessive processing of the complainant's personal data by means of a CCTV camera in a staff canteen.

Data controllers are tempted to use personal information captured on CCTV systems for a whole range of purposes. Many businesses have justifiable reasons, usually related to security, for the deployment of CCTV systems on their premises but any further use of personal data captured in this way is unlawful under the Data Protection Acts unless the data controller has at least made it known at the time of recording that images captured may be used for those additional purposes, as well as balancing the fundamental rights of employees to privacy at work in certain situations, such as staff canteens and changing rooms.

Case Study 8:
Disclosure of personal information to a third party by the Department of Social Protection

This Office received a complaint in July 2014 concerning an alleged unauthorised disclosure of the complainant's personal information by the Department of Social Protection to a third party. The complainant informed us that, in the course of an Employment Appeals Tribunal hearing, her employer produced to the hearing an illness-benefit statement relating to her. The statement contained information such as her name, address, PPSN, date of birth, bank details and number of child dependants. She stated that her employer was asked how he had obtained this illness-benefit statement. He stated that he had phoned the Department of Social Protection and the statement had subsequently been sent to him by email. Prior to making the complaint to this Office, the complainant had, via her solicitors, received an apology from the Department, who acknowledged that her information had been disclosed in error and that proper procedures had not been followed. However, she informed us that she had very little information as to how the disclosure had occurred and that the matter had caused her considerable distress.

We commenced an investigation by writing to the Department of Social Protection. In response, it stated that it accepted that a statement of illness benefit was disclosed to the complainant's employer in error, on foot of a telephone call from the employer. The Department acknowledged that the information should not have been sent out to the employer and that the correct procedures were not followed on this occasion. It stated that the staff member who supplied the information was new to the Department. It explained that it was not normal practice to issue a screenshot to the employer; the correct procedure was to issue a statement to the employee along with a note informing the employee that the information had been requested by their employer.

The data subject chose not to accept an apology from the Department as an amicable resolution of her data protection complaint, opting instead to seek a formal decision of the Data Protection Commissioner.

A decision of the Data Protection Commissioner issued in October 2015. In her decision, the Commissioner formed the opinion that the Department of Social Protection contravened Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003 by the further processing of the complainant's personal data in a manner incompatible with the purpose for which it had been obtained. The contravention occurred when the Department of Social Protection disclosed the complainant's personal data to an unauthorised third party.

This case serves as a reminder to data controllers of the importance of ensuring that new staff are fully trained and closely supervised in all tasks, particularly in those tasks that involve the processing of personal data. Errors by staff present a high risk of data breaches on an ongoing basis and it is critically important that efforts are made to mitigate against those risks by driving data protection awareness throughout the organisation, with particular focus on new or re-assigned staff

Case Study 9:
Covert CCTV installed without management knowledge

This Office received a complaint from staff of Letterkenny General Hospital in relation to the operation of covert CCTV surveillance by management within the Maintenance Department of Letterkenny General Hospital.

We also received a 'Data-Breach Incident Report' from the Health Service Executive (HSE) about this matter. This breach report recorded the incident as 'Unauthorised CCTV Surveillance of Office Area' and stated that a covert CCTV camera was installed by two maintenance foremen in their two-man office due to concerns they had in relation to the security of their office.

We commenced an investigation of the complaint by writing to the Health Service Executive (HSE), outlining the details of the complaint. We sought information from it in relation to the reporting arrangements between the maintenance staff in Letterkenny General Hospital and the maintenance foremen who installed the covert CCTV; the whereabouts of footage captured by the covert CCTV; the outcome of the internal investigation; how the covert CCTV was installed without notice to the management of Letterkenny General Hospital; and details of any instruction or notification issued to staff on foot of the internal investigation.

In response, the HSE stated that the foremen who had installed the camera were direct supervisors of the maintenance department staff and that the footage recorded was stored on a DVD and secured in a locked safe. It further stated that an internal investigation concluded that two staff had installed the covert CCTV without the authority, consent or knowledge of the management of Letterkenny General Hospital, due to concerns regarding unauthorised access/security in their office. We established that the camera in question was previously installed in a now disused area of the hospital, had been decommissioned and was re-installed in the office in question.

As well as confirming that the footage captured by the covert camera was of normal daily comings and goings to the maintenance office, the HSE stated that this was an unauthorised action by staff in the maintenance section and that it was keenly aware of its duty to all staff to provide a workplace free from unauthorised surveillance. The HSE confirmed that it would initiate steps to ensure that there would be no repetition of this action.

The HSE subsequently issued a written apology to the complainants in which it also confirmed that the recordings had been destroyed.

A decision of the Data Protection Commissioner issued in April 2015. In her decision, the Commissioner formed the opinion that the HSE contravened Section 2(1)(a) of the Data Protection Acts 1988 and 2003 by failing to obtain and process fairly the personal data of individuals whose images were captured and recorded by a covert CCTV camera installed without its knowledge or consent.

Covert surveillance is normally only permitted on a case-by-case basis, where the data is kept for the purpose of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This implies that a written specific policy must be put in place detailing the purpose, justification, procedures, measures and safeguards that will be implemented in respect of the covert surveillance, with the final objective being an active involvement of An Garda Síochána or other prosecutorial authority. Clearly, any decision by a data controller to install covert cameras should be taken as a last resort after the full exhaustion of all other available investigative steps.

Case Study 10:
Danske Bank erroneously shares account information with third parties

We received a complaint against Danske Bank alleging that it had disclosed personal data and account information in relation to a mortgage on a property owned by the complainant to third parties. We commenced an investigation of the matter by writing to Danske Bank, outlining the details of the complaint. We received a prompt response from Danske Bank, which stated that the complainant and the individual who received his personal data were joint borrowers on certain loan facilities and that it was during the course of email communications with the other individual in respect of that individual's loan arrears that the personal data relating to the complainant was disclosed to two third parties.

Danske Bank admitted that this was an error on its part and stated that it was unfortunate that it had occurred. It went on to explain that, in dealing with the queries raised by the other individual in respect of his arrears and entire exposure to Danske Bank, the relationship manager also included information on all arrears in respect of that individual's connections, which included the complainant. The staff member concerned expressed his regret at the incident and Danske Bank confirmed that the staff member was reminded of its procedures with regard to data protection and the need to be vigilant when dealing with the personal data of customers. Danske Bank apologised for the incident and offered reassurance that it would endeavour to prevent a future reoccurrence.

Danske Bank went on to state that it had robust controls in place to ensure that such incidents did not occur; however, it admitted that, despite such controls, this was a case of a human error and it did not believe that it was in any way intentional.

The complainant requested that the Data Protection Commissioner issue a formal decision on his complaint. A decision of the Commissioner issued in January 2015, and it stated that, following the investigation of the complaint, she was of the opinion that Danske Bank contravened Section 2(1)(d) the Data Protection Acts 1988 and 2003 by disclosing the complainant's personal data to a number of third parties without his knowledge or consent.

This case is illustrative of the need for financial institutions to be vigilant when dealing with the personal data of individuals who have common banking relationships with others, and to ensure that appropriate safeguards are in place to prevent accidental or erroneous sharing of personal data.

Case Study 11:
Failure to update customer's address compromises the confidentiality of personal data

This Office received a complaint that Allied Irish Banks (AIB) failed to keep the complainant's personal data up-to-date over a prolonged period, despite repeated requests by the individual to do so, and that it failed to maintain the security of the individual's personal information. The complainant informed us that he had repeatedly asked AIB to update his address details but that it had failed to do so. As a result, his correspondence from AIB continued to be sent to a previous address. The complainant alleged that, arising from the failure of AIB to update his address, his correspondence containing his personal data, which was sent to his previous address by AIB, was disclosed to unknown third parties at this previous address.

We commenced an investigation of the matter by writing to AIB, outlining the details of the complaint. AIB confirmed to us that, due to a breakdown in internal processes, the complainant's correspondence address was had not been updated on all its systems in a timely manner, resulting in automated arrears letters continuing to issue to an old address.

In circumstances where AIB had been advised that the complainant had changed address, our investigation was satisfied that its continued sending by post or delivering by hand of correspondence intended for the complainant to the previous address failed to secure the complainant's personal data against unauthorised access by parties who had access to the letterbox at the previous address.

Efforts to resolve the complaint by means of an amicable resolution were unsuccessful and the complainant sought a formal decision. In her decision, the Commissioner formed the opinion that AIB contravened Section 2(1)(b) of the Data Protection Acts 1988 and 2003 by failing to keep the complainant's personal data up to date.

This contravention occurred when AIB failed to remove the complainant's previous address from his account despite notification from him to do so. The Commissioner also formed the opinion that AIB contravened Section 2(1)(d) by failing to take appropriate security measures against unauthorised access to the complainant's personal data by sending correspondence by post and by hand delivery to an address at which he no longer resided, while knowing that this was no longer his residential address.

This case demonstrates the need for all data controllers to ensure that personal data is kept accurate and up-to-date at all times. Failure to do so may result in the disclosure of personal data to unauthorised persons as well as unnecessary distress and worry for data subjects who have updated the data controller with the most accurate information, only to find that the necessary safeguards were not in place to prevent their personal data being compromised by use, as in this case, of a previous address.

Case Study 12:
Unfair use of CCTV data

The subject matter of this complaint was the use by the data controller of CCTV footage in a disciplinary process involving one of its drivers. The data controller, Aircoach, advised that it was reviewing CCTV footage from one of its coaches as part of dealing with an unrelated customer-complaint issue when it happened to observe a driver using her mobile phone while driving a coach.

As is often the case with such complaints, the complainant objected to the use of the CCTV footage as evidence in a disciplinary process that was taken by Aircoach against her, the basis of the objection being that it was unfairly obtained.

Aircoach informed us that it had introduced CCTV across its fleet in order to further enhance safety and security for both staff and customers.

It further advised that all staff are informed that CCTV is installed and of the reasons behind its use, but admitted that it was not until the middle of 2014 that significant efforts were made to fully inform both staff and customers as to the presence of CCTV on its coaches. Aircoach provided us with a copy of its new CCTV policy and it also provided us with photos showing the CCTV signage on the coach entrance doors, adding that the process of putting appropriate signage in place on its coaches commenced in January 2014 and was concluded by October 2014.

The law governing the processing of personal data, including CCTV images, is provided for under Section 2 of the Data Protection Acts 1988 and 2003. Processing includes, among other things, the obtaining and use of personal data by a data controller and it must be legitimate by reference to one of the conditions outlined under Section 2A(1) of the Acts. In addition, a data controller must also satisfy the fair-processing requirements set out under Section 2D(1) of the Acts, which requires that certain essential information is supplied to a data subject before any personal data is recorded.

The investigation in this case established that, at the time of the relevant incident on 19 February 2014, the roll-out of CCTV signage by Aircoach had commenced; however, the company failed to properly or fully inform staff that CCTV footage might be used in disciplinary proceedings. Any monitoring of employee behaviour through the use of CCTV cameras should take place in exceptional cases rather than as a norm and must be a proportionate response by an employer to the risk faced, taking into account the legitimate privacy and other interests of workers. In this case, when processing the complainant's image, Aircoach was not aware of any particular risk presented and, by its own admission, was investigating an unrelated matter.

While it subsequently transpired that the incident in question was indeed a very serious matter, involving alleged use by a driver of a mobile phone while driving, there was no indication at the time of the actual processing that this was the case and the processing therefore lacked justification. In addition, the fair-processing requirements set out in Section 2D were not fully met and fair notice of the processing for the specific purpose of disciplinary proceedings was not given to drivers whose images might be captured and used against them. In those circumstances, the processing could not be said to have been done in compliance with the Acts and the Commissioner found that Section 2(1)(a) had been contravened.

It is important to note that the processing of CCTV images in disciplinary proceedings against an employee is very much circumstance-dependent. Thus, while on this occasion the employer was found to have been in contravention of the Acts because the images were processed without justifiable cause or fair notice to the employee in question, in other circumstances the processing might be regarded as being proportionate and fair, especially if the processing is done in response to an urgent situation and the employer has the correct procedures in place. Employers should therefore be careful to ensure that a comprehensive CCTV policy is in place and followed if they wish to stay within their legal obligations.

PRESENTATIONS AND ENGAGEMENTS WITH STAKEHOLDERS

In 2015, the Commissioner and her staff maintained an ongoing outreach schedule and actively engaged with a broad base of stakeholders. This included meetings with representatives of the many technological, social media and internet multinationals based in this jurisdiction, as well as attendance at numerous industry events. In addition, to increase the visibility and accessibility of the Office, the Commissioner and her staff also gave presentations at seminars, conferences and to individual organisations, including public-sector bodies, on over 60 occasions during the course of the year. Examples include:

- IDA Ireland Annual Conference
- Institute of International and European Affairs (IIEA) Conference on Data Protection and Privacy in the Digital Age
- IAPP Global Privacy Summit, Washington DC
- Spring Conference of European Data Protection Authorities, Manchester
- Public Affairs Ireland Data Protection Conference
- National Data Summit of Big Data Analytics
- Waterford Taking Care of Business Event
- Interdepartmental Committee on Data Protection
- Irish Centre for European Law and the Irish Bar Council Event on Regulatory Priorities under a Better Resourced Data Protection Regime
- Annual International Conference of Privacy Laws and Business, Cambridge
- Department of Children and Youth Affairs 'Growing up in Ireland' Research Ethics Committee
- Department of the Taoiseach State-sponsored Bodies Awareness Event
- UCD Masters of Law Class
- Credit Union Managers Association Seminar
- Department of Public Expenditure and Reform Graduate Development Programme
- European Data Protection Supervisor Staff Event
- ISACA – Ireland Chapter AGM

REGISTRATIONS STATISTICS

Certain categories of data controllers are legally bound to register with the Data Protection Commissioner on an annual basis. Section 16(1) of the Data Protection Acts 1998 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).

Data controllers may also be exempt from registering under the provisions of Regulation 3 of SI 657 of 2007. However, these exemptions need to be examined in conjunction with Regulation 4 of SI 657 of 2007, which sets out the categories of data controller who are always required to register. If a data controller is specified under Regulation 4, the exemptions listed under Regulation 3 of SI 657 of 2007 do not apply.

However, every data controller, regardless of whether they are required to register, is bound by the data protection responsibilities set out in the Data Protection Acts 1988 and 2003. Equally, registration is a separate legal process and 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

The total number of register entries in 2015 was 6,235. This figure can be broken down into the following categories:

Category	Number
Financial and credit institutions	591
Insurance organisations	322
Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts	78
Telecommunications/internet providers	58
Health sector	2,207
Pharmacists	1,137
Miscellaneous	447
Data processors	1,395

Total number of registration entries

2013	2014	2015
5,778	6,196	6,235

In 2015, the number of organisations registered increased by 39, an increase of approximately 0.6%.

ACCOUNT OF INCOME AND EXPENDITURE

Account of receipts and payments in the year ended 31 December 2015

	2015	2014
Receipts	**€**	**€**
Moneys provided by the Oireachtas	2,961,190	2,274,438
Fees	670,307	715,697
	3,631,497	**2,990,135**
Payments		
Staff costs	1,988,987	1,654,900
Establishment costs	283,396	73,115
Legal and professional fees	549,365	522,145
Auditors fees	4,600	4,117
Miscellaneous expenses	134,842	20,161
	2,961,190	**2,274,438**
Payment of receipts for the year to the Vote for the Office of the Minister for Justice and Equality	648,073	415,347
Receipts payable to the Vote for the Office of the Minister for Justice and Equality at year end	22,234	300,350
Total	**3,631,497**	**2,990,135**

ENERGY REPORT

Overview

Dublin
The DPC opened its Dublin base, complementing the existing Portarlington location, in mid-2015. Temporarily situated in the Regus Building, Harcourt Road, Dublin 2, it is expected that the team will move to a permanent Dublin location in mid-2016, and full energy reports will be provided going forward.

Portarlington
The DPC's Portarlington base is located on the upper floor of a two-storey building built in 2006 with a floor area of 13.38 square metres. At end 2015, 28 members of staff were accommodated in this area.

In 2015, the sources of the main usage of energy in the Office were gas and electricity for heating, lighting and other uses.

In 2015 the energy rating for the building was C1.

Actions Undertaken
The DPC has participated in the SEAI online system in 2015 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 2015:

Usage	**84,991.25 KWH**
Non-Electrical	44,631.25 KWH
Electrical	40,360 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.

NOTES

NOTES

Canal House
Station Road
Portarlington
Co. Laois
Ireland

Lo Call Number 1890 252 231
Telephone +353 57 868 4800
Fax +353 57 868 4757
E-mail info@dataprotection.ie

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner