An Coimisinéir Cosanta Sonraí / Data Protection Commissioner

Twenty-Fifth Annual Report of the Data Protection Commissioner 2013

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

Contents

List of tables and figures

Part 1

Foreword

2013 was the year of Edward Snowden, the NSA Contractor who revealed the extent of access by US and European intelligence agencies to personal data held by major internet and telecommunications companies. The revelations provoked a long-overdue debate on the proper balance in a democratic society between the protection of personal data and the obligation on governments to take measures against those who would use these services to further criminal objectives. The disclosures have already led to commitments by the US Administration to rein-in the activities of US intelligence services. They have also led to a re-examination of data flows between the EU and the USA under the "Safe Harbour" agreement.

The resulting debate has thrown a welcome spotlight on the general issue of State access to personal data. The recent decision of the Court of Justice of the European Union to invalidate the Data Retention Directive has clearly set out the need for proportionality in this area. The lack of such proportionality led my predecessor, Joe Meade, to take enforcement action against the initial Irish data retention regime, action that has now been vindicated by the CJEU judgment. The CJEU judgement also shows the importance of challenging such privacy-destroying measures, as was done in this case by Digital Rights Ireland, supported by the Irish Human Rights Commission.

But the CJEU judgment has significance beyond that of data retention. Our audits of State organisations have, in too many cases, shown scant regard by senior management to their duty to safeguard the personal data entrusted to them – a duty that is all the greater because of the legal obligation to provide such personal data to the State. Laudable objectives such as fraud prevention and greater efficiency must

meet a test of proportionality in the manner in which personal data is used. Failure to treat personal data with respect can only lessen the trust that should exist between the individual and the State. It will also lead inevitably to more formal enforcement action by my Office unless system-wide action is taken to improve current practice.

Trust is also essential between the individual customer and commercial entities. As explained later in the Report, many of the complaints we deal with are as a result of poor standards of customer service. The fact that we have to take enforcement action for repeat failures in this area is a source of concern.

We remain willing to assist organisations in any way we can to achieve higher standards of data protection. Our audits are part of this effort. We continue to prioritise for audit the increasing number of information-rich multinational companies that have chosen Ireland as a base for providing cross-border services.

As we face into a new and challenging era of data protection, with strengthened EU-wide legislation, I wish again to thank the staff of our Office who continue to do their often challenging work with cheerful commitment.

Billy Hawkes
Data Protection Commissioner
Portarlington, May 2014

Introduction

Late 2012 saw the recruitment of additional staff - including specialist posts of Technology Advisor and Legal Advisor - to deal with the increased responsibilities arising from our oversight of multinational companies providing services across the European Union from their Irish establishments. Nevertheless, the activities of domestic data controllers - both in the private and public sectors - continued to attract the great bulk of enquiries and complaints in 2013.

We continued to devote significant resources to our advisory function, preferring to assist organisations to achieve best practice in data protection rather than having to deal with non-compliance issues. Our audit activity continued to target a balanced range of multinational and domestic data controllers. In relation to State organisations, we have now completed audits of 3 major holders of personal data - the Department of Social Protection, the Revenue Commissioners and An Garda Síochána (national police force). We also achieved an increase in the number of organisations registered with our Office, largely through targeted enforcement action.

Allocation of Resources

Note: Staff costs = 82% of Budget

Investigations & Enforcement[1] 35%

Guidance & Education[2] 25%

Audits/Inspections 15%

Notifications[3] 10%

EU/International Cooperation 10%

Administration[4] 5%

[1] Includes investigating complaints and data breaches ; issuance of Enforcement Notices ; prosecuting offences under the Data Protection Acts and the Electronic Privacy Regulations

[2] Includes Help-Desk ; oral and written guidance to organisations (including meetings) ; presentations and other public education activities

[3] A limited number of organisations are required to register annually with the Office. Information on the types of information they process etc is provided in the Register on the Office's website

[4] Back-office services (IT, HR, Finance) are handled by the Department of Justice and Equality

Customer Service

This year, once again, the Office continued to provide services to our customers, both data controllers and data subjects, by phone, in person, by email and by post. We responded to large numbers of phone calls to our Helpdesk from members of the public on a very broad range of issues, from access rights to registration obligations. Emails were the next most common method of contact. Approximately 12,000 queries were dealt with in 2013 via our dedicated information email address – info@dataprotection.ie, an increase from 9,500 the previous year. In addition we received queries by post.

Our practice of involving the entire staff of the Office in providing service on our helpdesk, which we started in late 2006, has continued with great success. The benefit to members of staff providing this service is a greater awareness of the data protection issues facing members of the public and organisations alike.

The website remains our main source of public information which we review and update regularly to make sure that relevant data protection developments are highlighted to visitors to it.

During 2013, we gave 72 presentations to various organisations, details of which are available in Appendix I – Presentations and Talks.

Media Relations

Interaction with the media provides a valuable platform for raising awareness among the public on data protection issues. Last year the Office dealt with over 450 queries from national and international media outlets. Numerous press releases and other website notices issued during 2013 dealing with matters which were the subject of ongoing investigation and other matters to which the Commissioner wished to draw public attention.

Irish Language Scheme

Our second Irish Language Scheme under the Official Languages Act 2003 fell for review during 2013. Submissions were sought from the public in relation to the drafting of the third Scheme. We continue to maintain our commitment to provide a comprehensive service in the Irish language to our customers, including by providing comprehensive information on our Irish language website, www.cosantasonrai.ie.

Governance

A Revised Code of Practice for the Governance of State Bodies was issued on 9th June 2009 by the Department of Finance and was circulated to all Heads of Agencies. It is mandatory for all State bodies.

The Office utilises core systems and services provided by the Department of Justice and Equality – payroll, general payments, travel bookings, HR, and IT (Citrix) – which are subject to that Department's procedures. The Office is also subject to the Department's internal audit system. Insofar as matters under its control are concerned, the Office is in full compliance with the requirements of the Code.

Complaints and Investigations

During 2013 this Office opened 910 complaints for investigation. This compares with 1,349 complaints in 2012 (369 complaints of the 2012 total related to one particular matter).

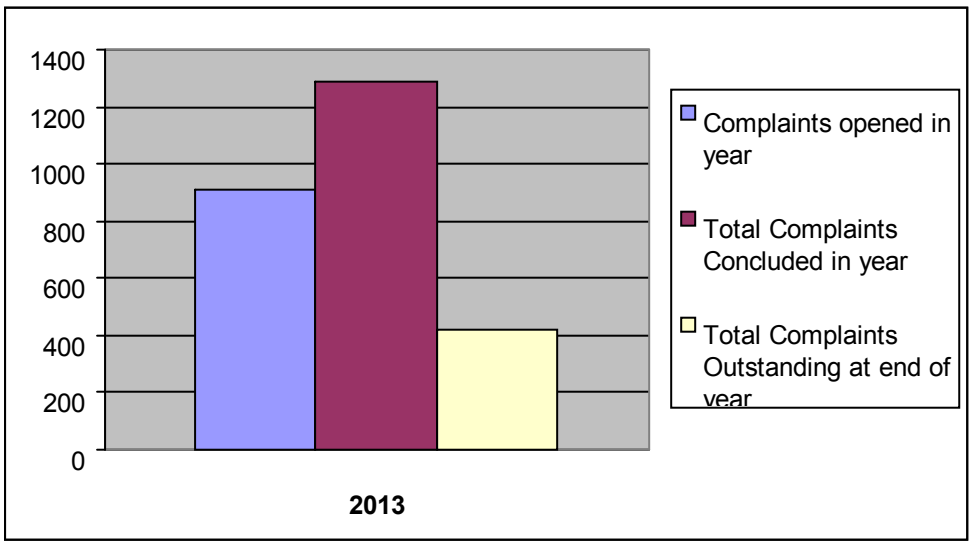
Complaints concerning access requests accounted for 56.8% of the overall total for 2013. With 517 individual complaints received in relation to access requests, this was the highest number ever received by the Office in this category. On the one hand this is indicative of the increased level of awareness among the general public of their statutory right of access. However, the complaint levels also point to the extent of the difficulties being experienced by individuals in their efforts to exercise their rights and the barriers that some data controllers place in their way. As a result of such difficulties, data subjects must seek the intervention of this Office to assist them in exercising their rights. That individuals experience difficulties in what should generally be a straightforward exercise is disturbing and it reflects poorly on data controllers who fail to fully comply with their obligations.

The number of complaints under the Privacy in Electronic Communications Regulations (S.I. 336 of 2011) in 2013 was 204 (22.4% of the overall total). These complaints related to unsolicited direct marketing text messages, phone calls, fax messages and emails. The 2013 figures in this category are somewhat similar to recent years - with 606 such complaints in 2012 (369 of which related to one particular matter as indicated above), 253 in 2011, 231 in 2010 and 262 in 2009. Breaches of the Regulations may be prosecutable offences. The Commissioner frequently uses his prosecution powers against entities who continue to infringe the law. The Case Studies section of this Annual Report carries details of the prosecutions taken in 2013 for offences committed in respect of breaches of the Regulations. Once again, the Commissioner is reporting this year on prosecutions taken against some of the major companies in the telecommunications sector in relation to marketing offences. It is disappointing that this sector remains a cause of complaint to this Office given the number of prosecutions taken against companies in that sector in recent years and in light of the fact that the players in this sector are well aware of the data protection law and have internal data compliance units to promote a culture of compliance. It

appears, on the basis of complaints received, that a lot of compliance work remains to be done in that sector.

The vast majority of complaints concluded in 2013 were resolved amicably without the need for a formal decision under Section 10 of the Acts, or enforcement action. In 2013 the Commissioner made a total of 29 formal decisions. 25 of these fully upheld the complaint, 1 partially upheld the complaint and 3 rejected the subject of the complaint. A total of 1290 investigations of complaints were concluded in 2013 (Figure 1).

Figure 1 Complaints



	2013
Complaints opened in year	910
Total Complaints Concluded in year	1290
Total Complaints Outstanding at end of year	418

Table 1 shows the breakdown of complaints by data protection issue. Excluding the 204 complaints (approx 22.4%) concerning breaches of S.I. 336 of 2011, the remainder (approx 77.6%) relate to breaches of the Data Protection Acts, 1988 & 2003. Table 2 gives details of the number of complaints received on an annual basis since 2004.

Table 1 Breakdown of complaints opened

2013 Breakdown of complaints by data protection issue

	2013 Percentages	Totals
Access Rights	56.8%	517
Electronic Direct Marketing	22.4%	204
Disclosure	6.9%	63
Unfair Processing of Data	3.8%	35
Unfair Obtaining of Data	2.3%	21
Use of CCTV Footage	1.8%	16
Failure to secure data	1.3%	12
Accuracy	1.1%	10
Excessive Data Requested	1.1%	10
Right of Rectification	1.0%	9
Unfair Retention of Data	1.0%	8
Postal Direct Marketing	0.3%	3
Other	0.2%	2
TOTALS	100.0%	**910**

Table 2 Complaints received since 2004

Year	Complaints Received
2004	385
2005	300
2006	658
2007	1037
2008	1031
2009	914
2010	783
2011	1161
2012	1349
2013	910

Use of Statutory Enforcement Notices

Details of Enforcement Notices and selected Information Notices served in 2013 are set out in the following tables. Most relate to the right of access. It is to be hoped that publication of these lists encourages all organisations that are the subject of complaints to co-operate fully with our Office in relation to our 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.

Table 3 - Enforcement Notices* issued in 2013

Data Controller:	In relation to:
Hellweek PT	Section 2A(1)a and 2D(1) of the Data Protection Acts
Ian Mallon Solicitors	Section 4(1) of the Data Protection Acts
PPI Claimback Limited	Section 4(1) of the Data Protection Acts
Flightwise Training Services Limited	Section 4(1) of the Data Protection Acts
Irish Prison Service	Section 4(1) of the Data Protection Acts
Westwood Club Limited	Section 4(1) of the Data Protection Acts
Loyaltybuild Limited	Section 2(1)(d) of the Data Protection Acts
Musgrave Group	Section 2(1)(d) of the Data Protection Acts
Axa Insurance Limited	Section 2(1)(d) of the Data Protection Acts
Nordon Landscapes	Section 4(1) of the Data Protection Acts

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

Table 4 - Selected Information Notices* issued in 2013

Data Controller:

The Five Lamps, Naas

ESB Electric Ireland Ltd

*Under Section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a person to provide him with whatever information the Commissioner needs to carry out his function, such as to pursue an investigation.

Access Request Complaints

In 2013 this Office opened for investigation 517 complaints from individuals who experienced difficulties in accessing their personal data using their right of access under Section 4 of the Data Protection Acts, 1988 and 2003. This figure represented 56.8% of the overall total of complaints which we opened for investigation. The number of access requests complaints opened for investigation in the previous four years were as follows:

2012 - 442
2011 - 562
2010 - 308
2009 - 259

In summary, over the past five years we have opened over two thousand complaints concerning access requests for investigation and, in that time, the number of complaints to this Office concerning access requests has doubled (from 259 in 2009 to 517 in 2013).

While, on the one hand, the increased number of complaints is indicative of increased awareness on the part of individuals of their right of access and increased activity on the part of individuals in actually exercising that right, our investigations of those

complaints points to certain issues that we wish to draw attention to in this Annual Report.

Customer Service Issues

The purpose behind the making of access requests to data controllers in many cases is often a customer service issue which has been badly handled by the data controllers concerned in the first instance. Time and again we find in our investigations customers or clients who believe they have been treated badly in their dealings with a company or entity and who, despite their best efforts, are unable to find adequate redress in pursuing the matter from a customer service perspective. Having failed on that front, they resort to submitting access requests to obtain a copy of all personal data held on them by the data controller concerned. For the data controller's part, the issue moves internally from the customer service department to the data compliance department and a significant amount of time and resources may be expended on processing the access request. With increasing frequency we are finding in our investigations that shortcomings in the handling of customer service complaints, or indeed bad customer service in the first instance, is the driving force behind many access requests. By not properly or adequately dealing with the customer service issue, the company or entity concerned often finds itself having to process an access request in addition to having to deal with the customer service issue. The processing of an access request can be a time and resource consuming exercise, particularly where the data controller concerned holds a significant amount of personal data about the requester. In our view, every organisation which is in receipt of significant numbers of data access requests should seriously examine the underlying cause of such requests to establish if its level of customer service (or indeed failures in delivering customer service) is a significant contributory factor. If so, it should strive to take remedial action to ensure that its customers or clients do not feel obliged to exercise their right of access in order to achieve a satisfactory level of customer service. It follows that good customer service and an effective customer service complaints mechanism will relieve the overall administrative burden for the company or entity concerned and it will assist the customer or client concerned in achieving redress in a timely manner.

Telephone Call Recordings

We have seen an increase in the number of access requests to data controllers by individuals seeking a copy of telephone call recordings. It is important that data subjects and data controllers note the following in relation to seeking call recordings under Section 4 of the Data Protection Acts.

- Telephone call recordings constitute personal data insofar as they contain information related to the persons on the call.

- An access request which seeks a copy of a telephone call recording should be specific as to the time and date of the call. If it is not specific, the data controller may rely on the provisions of Section 4(3) of the Data Protection Acts to seek from the requesting data subject further information to assist it in locating the call recording(s) concerned. For example, the data subject may be asked to provide details of the date of the call(s), the approximate time(s) of the call recording being sought and, if necessary, the phone number from which the call was made and the phone number to which the call was made.

- Organisations must inform data subjects if a call recording system is in operation and that calls may be recorded.

- Data subjects should be aware that organisations which operate a call recording system may not record every telephone call. In some cases, calls are randomly recorded. Obviously, if a telephone call was not recorded then the data controller would be unable to provide a copy of it. Data controllers are obliged to give requesting data subjects a copy of the personal information only which they hold and that is the extent of it. However, we encourage data controllers to be upfront in declaring in their privacy policies, their procedures in terms of call recordings and how such recordings may be accessed. By so doing, confusion and complaints about the matter may be avoided.

- Data controllers must have in place a retention policy in relation to any call recordings.

Data Breach Notifications

During 2013, the Office dealt with 1,577 personal data security breach notifications. Of this figure, 70 were deemed not to be personal data security breaches on the part of the data controller making the notification. A total of 1,507 valid data breach notifications were therefore recorded.

In our report of last year, we listed a case study (No. 15) regarding procedures AIB were implementing to deal with the issue of changes of address not being correctly recorded, leading to disclosures of personal data via post. This Office is pleased to note that the actions carried out by AIB have resulted in a significant reduction of the number of notifications made during 2013.

The data security breach at Loyaltybuild Ltd, towards the end of 2013, had a very high media profile and involved a resource intensive response from the Office, both in terms of the investigation and keeping the general public informed of developments. A report of the investigation is included as Case Study 14.

An EU Regulation, Commission Regulation 611 of 2013, came into effect across the EU on the 25th August, 2013. This Regulation sets out specific rules for the notification of data security breaches by Telecommunications and Internet Service Providers. It requires that notifications are made to the relevant national authority within 24 hours of a data security breach being identified. Where a service provider is not in a position to make a full report at that time, an initial report can be made, but a full report must be made within 72 hours of the initial notification, or an explanation as to why such a report can not be furnished at that time.

The Regulation also imposes a requirement on the relevant national authority to provide a secure form through which a service provider can make such a notification. This Office, as the relevant national authority, has provided this form via our website.

Another issue that was highlighted in last year's Annual Report was the beginning of a trend of notifications to this Office regarding the issue of staff moving from one employer to another and taking client data to their new employer. We received a number of such notifications in 2013. Our Office, in dealing with one such breach notification, exercised its powers under Section 24 of the Data Protection Acts to carry out a site inspection of one data controller (see Case Study 15).

Our Office also received a number of personal data security breach notifications that involved data subjects from other countries. These notifications are coming from large tech corporations who have established a base here in Ireland and also native businesses who are offering services across the globe. This is leading to our Office cooperating more closely with other Data Protection Authorities in the investigation of such security breaches.

Our Office, in line with our desire to work effectively with other Data Protection Authorities, instigated joint investigations into breach notifications made to this Office with the Privacy Commissioner of Canada. The investigations, which are ongoing at the time of publication of this Report, involve notifications received from Adobe Software Systems Ireland and Facebook Ireland.

The nature of data security breaches being reported is also changing. This Office is finding it necessary to liaise with other organisations to properly understand the impact of some breaches and also to determine what would be an appropriate course of action to be taken by the data subjects to protect themselves from harm. Case Study 16 shows how we interacted with the Passport Office to determine the actual risks to affected individuals and what steps could be taken to protect them. In dealing with the Loyaltybuild breach investigation (Case Study 14), we interacted with the various banks to determine what course of action they would take. We also discussed with the Irish Payment Service Organisation (IPSO) the potential risks and the steps that would be taken by the Card Issuers. IPSO also provided valuable assistance in understanding the PCI-DSS[5] requirements of an organisation. The Loyaltybuild security breach also showed that in such circumstances a number of organisations would be involved in the

[5] Payment Card Industry – Data Security Standard

investigation and these organisations need to work together to ensure a successful investigation.

The Loyaltybuild breach investigation also saw this Office providing regular updates to Data Protection Authorities throughout Europe, because there were a number of data controllers in their jurisdictions affected by the data security breach.

Table 5 – Number of breach notifications received 2013

Total Number of Breach Notifications Received	1577
Number considered as non-breach	70
Number of Breach Notifications	1507

Table 6 – Number of Organisations making Breach Notifications, 2013

Private Sector Organisations	246
Public Sector Organisations	61

Table 7 – Breach Notifications - by Category

Category	Number
Theft of IT Equipment	23
Website Security	53
Mailing Breaches (Postal)	920
Mailing Breaches (Electronic)	151
Security	86
Other	274
Total	1507

Table 8 – Comparison of Breach Notifications – by Year

2009	60
2010	410
2011	1167
2012	1592
2013	1507

Table 9 – Comparison of Organisations making Breach Notifications

Year	Private Sector	Public Sector	Total
2009	60	26	86
2010	89	34	123
2011	146	40	186
2012	220	84	304
2013	246	61	307

Figure 2 – Breaches by Category

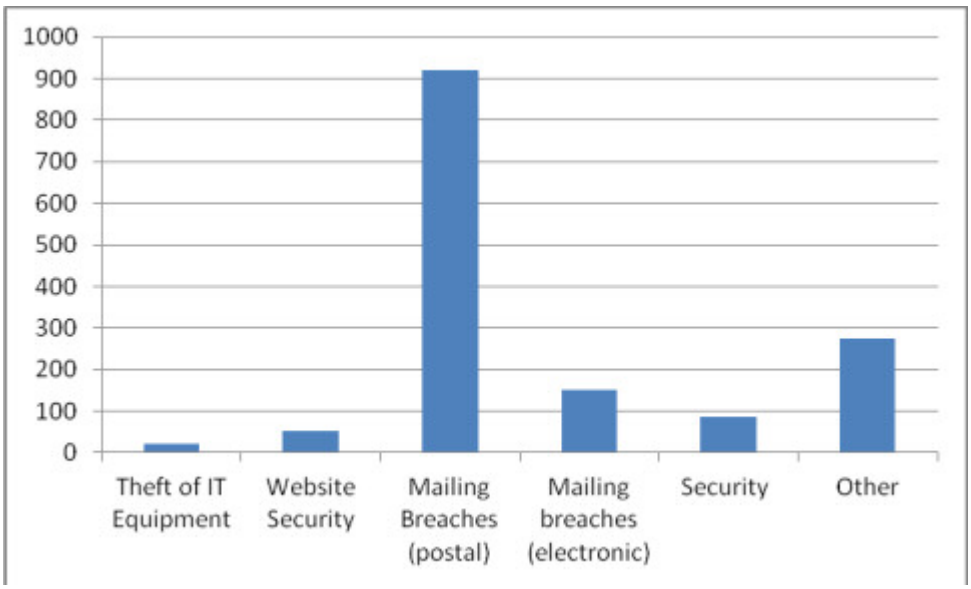


Figure 2 shows that again postal breaches account for the majority of notifications made to this Office. While a number of these are the result of mail merge issues at the printing stage, an unacceptably high percentage are the result of human error. Whether it is incorrectly recording the address or simply putting the wrong letter in the envelope, the affect on the individual can be distressing, especially where there is sensitive or financial data involved.

Privacy Audits

The Commissioner is empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Scheduled audits are intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive and are sometimes supplementary to investigations carried out by the Office in response to specific complaints. Priorities and targets for audit are identified taking account of factors such as the amount and nature of personal data processed by the organisation and complaints and enquiries to the Office. A particular priority is given to companies providing services cross-border from Ireland and to major holders of personal data in the public sector. During 2013, the Office continued to adopt a proactive role in this regard. In the course of the year, over 44 audits and inspections were carried out. The Office also continued with its programme of unscheduled inspections under powers conferred under section 24 of the Data Protection Acts.

As in previous years, the programme of audits was tailored to allow for a focus on a few carefully selected targets; in 2013 this entailed a focus on the completion of the An Garda Síochána audit report and an audit of LinkedIn-Ireland.

An Garda Síochána

The Office undertook an audit of data protection in An Garda Síochána (AGS) over the years 2011 to October 2013. The audit consisted of an examination of documentation provided by AGS, discussions with AGS senior management and on-site inspections at AGS HQ in Dublin, the AGS Vetting Unit in Thurles, the AGS Information Services Centre (GISC) in Castlebar and Garda stations in Donnybrook, Mullingar and Limerick.

The audit was carried out by reference to the requirements of the Data Protection Acts and the elaboration of those requirements contained in the ODPC-approved Data Protection Code of Practice for AGS. Full cooperation was received from AGS.

A central focus of the audit was the main IT system used by AGS for recording data, PULSE. This investigation involved detailed examination of the recording of data by the Garda Information Services Centre and by individual AGS members, the classification of such data and the systems in use to maintain the accuracy and security of the data and to prevent improper disclosure. The audit report describes in detail the procedures in place with regard to how certain personal data or episodes in an individual's dealings with AGS are recorded. Often, as evidenced during the audit, this entails the management by AGS of large unstructured formats of data. In the findings, we highlighted areas where improvements are required but equally we acknowledge practices and procedures where there were no data protection issues arising. Overall, we found that the majority of the areas examined demonstrated a professional police force operating in compliance with data protection legislation.

While the Office was generally satisfied with the in-built data protection mechanisms in PULSE, this was not the case in relation to the oversight of access by individual AGS members to records of individuals and the related risk of disclosure outside of AGS. The Audit Team came across disturbing instances of such improper access and found that scheduled audits of accesses to PULSE, as provided for in the AGS Data Protection Code of Practice, had not been carried out. However, implementation of that aspect of the Code had commenced by the time the audit ended. In addition, as a response to the inappropriate access detected during the audit, AGS instigated a three-pronged approach to counter any future inappropriate access namely HQ Directive 95/2012 "Data Protection in An Garda Síochána", a revised warning notice on PULSE displayed to all users as they log on and a programme of random audits conducted by the Garda Professional Standards Unit. The Commissioner expects An Garda Síochána to now actively enforce the terms of HQ Directive 95/2012 and take strong and appropriate disciplinary action against any persons abusing their access to PULSE and prosecutions against any person found to be using such access for gain.

We examined the processes in use to respond to requests from employing organisations in authorised sectors for vetting of employees and requests from individuals for access to their personal data. We considered that a fundamental area requiring clarification by AGS to data subjects is to outline clearly what will be

disclosed back by AGS via an authorised signatory to an organisation for vetting purposes as opposed to what a data subject can expect to receive via a subject access request made to AGS under section 4 of the Data Protection Acts. This is the source of frequent enquiry to this Office when a data subject or their solicitor makes an access request to AGS and views the content supplied in response by AGS. Both processes rely heavily on the accuracy of data contained in PULSE and the audit team was satisfied that both processes were subject to appropriate procedures, notably as regards data accuracy.

The audit included an examination of the processing of personal data in relation to the arrest and detention of individuals. Such processing is significantly determined by detailed statutory requirements, including those related to the taking of fingerprints and photographs. Failure to comply with such statutory requirements can result in difficulty in securing convictions in Court. No significant issues were encountered in this area.

An area of concern is the use for criminal investigation purposes of fingerprints of individuals required to provide such fingerprints in connection with applications for asylum, visas and residence. The Office indicated to AGS that we consider some practices in this regard raise issues from a data protection perspective and recommended that AGS revisit this issue with the Attorney General in the interests of clarity for all parties concerned taking account of the European legislative context.

We examined the processes in use for AGS access to subscriber data held by telecommunications companies and there were no data protection issues of concern arising in this regard.

The use of CCTV by AGS as well as the AGS Automatic Number Plate Recognition (ANPR) system was reviewed. There were some minor recommendations with regard to CCTV but no data protection issues of concern arising in regard to ANPR.

Other areas examined included the processing of data in relation to sex-offenders; AGS access to vehicle and driver information; data disclosures to 3rd parties; and

exchange of data with other countries. No significant issues were encountered in this area.

During the course of the various inspections, the audit team noted that AGS had not yet developed a comprehensive policy on data retention – one of the commitments contained in the Garda Síochána Data Protection Code of Practice. AGS committed to examining the organisational implications of the retention or deletion of all categories of personal data held by AGS.

Though not specifically raised in the course of the audit, this Office believes AGS should have a dedicated data protection unit, headed by an Officer with direct access to the Garda Commissioner. The Audit Report is available on the Garda website.

LinkedIn-Ireland (LinkedIn-I)

In 2013, we began a major audit of LinkedIn-Ireland. The on site element of the audit was conducted in May 2013 in LinkedIn-Ireland's European headquarters in Dublin. Intense systems testing and interaction with the Company continued throughout 2013. The audit report will be finalised in 2014. Already ahead of the completion of the audit report, LinkedIn-I have agreed to a wide range of "best practice" improvements.

Global Privacy Internet Sweep

At the beginning of the year the Office volunteered to participate in the Global Privacy Enforcement Network's (GPEN) Internet sweep along with Australia, Canada, Estonia, Finland, France, Five Regional DPA's from Germany, Hong Kong, Macao, Macedonia, New Zealand, Norway, UK, & USA. The GPEN Internet sweep was an exercise intended to review websites in the jurisdiction of each participating data protection authority in terms of the following criteria:

- Does the web site have a privacy policy?
- How difficult is it to find information about the site's privacy practices?

- Is contact information for addressing privacy questions and concerns readily available?
- How readable is the information about privacy practices?

In Ireland's case this involved the examination of 79 different websites based on internationally agreed scoring criteria.

The highest score available was 6 and 14 websites (17%) scored top marks. Those companies were: AA Ireland, ALDI, Awear Ireland, Carzone, Citizens Information, Eflow, Evening Herald, Groupon.ie, Irish Meteorological Service Met.ie, Marks and Spencer, Meteor, TG4, Three, Vodafone.

4 of the websites (5%) did not have a privacy statement and we took further action to ensure this was rectified immediately.

31 websites (39%) scored 4 or less and 48 websites (61%) scored 5 or more.

'Cookie Compliance' Sweep

In December 2012, the Office wrote to some 80 websites seeking information on the steps that they have taken to meet the so called "cookie" obligations placed upon them with effect from 1 July 2011 when Statutory Instrument No. 336 of 2011 (SI 336 of 2011) came into effect in Ireland. The revised rules for cookies are set down in Regulations 5(3) and 5(4) of SI 336 of 2011. Essentially, the rules provide that all websites must provide information and capture consent for dropping or accessing cookies or other information on a user's computer equipment when a user visits their site.

Throughout 2013, we engaged with these 80 websites to ensure they achieved compliance with the revised rules. As a result of this exercise, the Office produced revised guidance[6] to assist organisations whose websites deploy cookies to achieve at least a minimum standard of compliance: namely, prominent notification that cookies

[6] FAQ 5.3 http://www.dataprotection.ie/docs/Topical-Data-Protection-Issues/1241.htm

were being used and a link to a comprehensive statement on cookies including a listing of each of the types of cookie being dropped.

Organisations audited in 2013:

In the course of 2013, 44 audits and inspections were carried out by the Office. This is a 10% increase on the previous year – 2012 - in which 40 audits were completed in total. A range of desk-based audits were also conducted including a review of injury compensation websites.

The inspection teams found that there was a reasonably high awareness of, and compliance with, data protection principles in the organisations that were inspected. Notwithstanding this, the majority of organisations had areas where immediate remedial action was necessary. It was noted with satisfaction that the majority of the data controllers audited have demonstrated a willingness to put procedures in place to ensure they are meeting their data protection responsibilities in full. The Commissioner would like to thank all of the organisations audited and inspected throughout the year for their cooperation.

List of Organisations audited/inspected

European Customs Information System (CIS) – National Unit, Revenue Commissioners
Medicus Medical Centre
LinkedIn-Ireland
Panda Waste
Carlow Institute of Technology
AES Waste Management
Reads Print and Design
TenantReference.ie
Arnold & Green Liability Adjusters
AA Ireland
Glanbia
SIPTU
Matt Hall PI
Health & Safety Authority
Fines Collection Service
MJG Investigations Ltd
Duffy Amusements (issue specific)
Irish Life (issue specific)

An Post (issue specific)
Tower Plant & Civil Engineering Ltd (issue specific)
Dublin City Centre Citizens Information Service (issue specific)
Advanced Laser Light (issue specific)
M. Roche & Co Solicitors (issue specific)
New Look Hair and Beauty Bar (issue specific)
Dresses.ie-Sunwav Ltd (issue specific)
In Dublin -Seven Hats Media Ltd (issue specific)
St John's Credit Union Ltd
MPCC Credit Union Ltd
St. Mary's Parish Credit Union
St. Declan's Ashbourne Credit Union Limited
Balbriggan Credit Union,
Munster Soft Drinks Limited
IBRC
CityBus Employees' Credit Union
Loyalty Build
Meridian Services (Tracing) Ltd
Caherdavin & District Credit Union Limited
MJG Investigations
Portlaoise Credit Union Ltd
Portarlington Credit Union Ltd
Tullamore Credit Union Ltd
Monasterevan Credit Union Ltd
Athy Credit Union Ltd

Desk Audit of Injury Compensation websites

www.motorassist.ie

www.personalinjurysolutions.info

www.Accidentclaimsdirect.ie

www.Personalinjuryspecialist.ie

www.Mycase.ie

www.carmodymoran.ie

www.accident-claims-ireland.info

www.Personalinjuryireland.ie

www.Carcrash.ie

www.Solicitorsinireland.ie

www.claim.ie

www.personalinjuriesassessmentboard.com

www.irishclaims.com

www.injuriesboardadvice.com

www.injury-compensation.ie

www.personalinjurysolicitor.ie

http://www.injury-solicitors.ie/

www.injury-compensation-ireland.com

www.nowinnofeesolicitors.com

www.compensationireland.com

Policy Issues

STATE ACCESS TO COMMERCIAL DATA HOLDINGS

Previous annual reports have referred to our concerns about access by State organisations to personal data held by telecommunications companies under data retention legislation and the need for improved safeguards in this area. A challenge to the proportionality of the Irish legislation and to the EU directive on which it is partly based has been referred by the Irish High Court to the Court of Justice of the European Union, based on a case brought by an Irish NGO, Digital Rights Ireland, with the support of the Irish Human Rights Commission.

In the course of the year, this issue acquired an international dimension with the disclosure of extensive access by US and European intelligence agencies to personal data held by major internet and telecommunications companies. The revelations led to a call from the European Parliament for a suspension of the EU-US "Safe Harbour" agreement under which personal data can be transferred from the EU to the US. It also added increased emphasis to the publication by the European Commission of a series of recommendations addressed to the US authorities for improvement of US oversight of the Safe Harbour arrangement, including restrictions on access to transferred data by US intelligence agencies. A report on implementation of these recommendations is anticipated in mid-2014.

CCTV IN CRECHES

Following the broadcast of an episode of RTE's *Primetime* featuring practices in certain crèches in Dublin, this Office had a number of queries in relation to the provision of CCTV in crèches. Some crèches queried the possibility of live streaming of CCTV to parents, use of same by management and also the placing of CCTV cameras in all areas of crèches to reassure parents.

The position of the Office conveyed to the crèches in relation to the legitimacy and proportionality of the use of CCTV in a crèche environment, is that the Commissioner is satisfied that CCTV may be used legitimately under the Data Protection Acts for security related purposes at the perimeter of such a facility but that any use beyond this would need to be fully justifiable and evidence-based with a very high threshold for such evidence. This is particularly the case in a crèche environment as the majority of the personal data processed will relate to minors. We also commented that it may be the case that employers are tempted to use technologies such as continual streaming of CCTV as a substitute for on-the-ground supervision by supervisory or managerial staff. However, such situations are difficult to reconcile with the requirements of the Data Protection Acts and we cannot see any legal basis to justify the monitoring of individuals in the course of their normal activities by such means.

In essence CCTV cameras in crèches raises a range of data protection issues including the rights of parents who do not wish to have video surveillance in place as well as the rights of employees. This Office considers that CCTV is not an answer to the fundamental issues of the quality of staff and their supervision by management in a child-care facility.

SMS CAMPAIGNS BY CHARITIES

It became apparent to this Office in 2013 that a number of Irish Charities were using a new third party service provider to manage SMS fundraising campaigns on their behalf.

The Office acknowledges that it is perfectly legitimate for charities to seek to collect donations by means of an SMS service. Once a donor decides that they wish to contribute to the charity concerned by means of a text message (involving a deduction of the amount of the donation from the mobile phone account), they can proceed to do so in an easy manner by texting the advertised word to the five digit short code. In those circumstances, the minimum amount of personal data is required to be processed

in order to process the actual donation. Once the service provider / third party processor operating the short code notifies the relevant mobile phone company of the donation and the donation is then processed on the mobile phone account, there is no further data processing required. There is no obvious requirement for the charity concerned to receive anything other than the monetary donation in those circumstances and this Office would not expect the charity to receive details of the donating mobile phone number.

However, it came to the attention of this Office that the advertising used by some charities indicates that phone numbers will be added to a marketing/promotional database. This suggests processing of personal data of a more extensive nature and, in that context, the requirements of both the Data Protection Acts and SI 336 of 2011 must be met.

As far as data protection law is concerned, the use of the phone numbers of donors for further electronic contact, or to be put on a marketing database, may take place only where the phone subscriber concerned has actively opted in to such use of their phone number in the knowledge that it will be used to contact them for direct debit and /or marketing/promotional purposes. It is not acceptable or lawful for a charity to place a donor's phone number on a marketing database, solely on the basis that the phone subscriber concerned made a donation to the charity using the SMS method. Therefore advertising which states *"by texting you are consenting to be contacted by us"* (or wording of a similar nature) does not meet the requirements of the law. If a charity were to contact the donor's number or add the number to a marketing/promotional database on that sole basis and without specific 'opt in' consent, firstly the charity concerned would breach the Data Protection Acts by so doing and, secondly, if it were to make follow up marketing contact by text message or phone call to the donor concerned, it would commit a criminal offence under the Regulations (SI 336 of 2011) which apply to unsolicited electronic marketing communications.

Furthermore, a third party processor which carries out marketing campaigns (e.g. phone or text message / email campaigns) on behalf of the charities concerned could

themselves face prosecution if they target donors who have not unambiguously consented to the receipt of such communications or calls. As a result of interactions with a number of charities and a service provider in relation to the issue, this Office prepared a guidance note for both charities and members of the public in relation to these campaigns and published this guidance on our website.

INTRODUCTION OF NATIONAL POSTCODE SYSTEM[7]

This Office was consulted by the Department of Communications Energy and Natural Resources, in relation to a unique, seven character postcode[8] to be allocated to every home in the country in 2015. We had previously engaged with the Department on this issue in 2006 and again in 2010 when we expressed a serious concern that a public database linking a code to a single unit residential address could be considered as being personal data of the occupants of that dwelling. In the Irish context, a person's home address is an important part of their identity and is the second most important piece of personal information to verify a person's identity. Furthermore, in the case of a family home, a postcode could link many related individuals in the course of their daily activities.

In essence the unique seven character postcode goes beyond what an "address" is because, through the use of modern technology and "Big Data", it can be easily assimilated into any sort of electronic device or dataset which could in turn be used for any purpose, ranging from State services to commercial exploitation. In this regard, we expressed the concern that such datasets which would be verified by this postcode could have the potential for the ready identification of sensitive information about individuals, examples of which would be to identify specific localities that have patterns of crime or illness.

[7] See Section 66 of the Communication regulation (Postal Services) Act 2011
[8] "postcode" means a code consisting of numbers or other characters or both numbers and other characters that identifies the locality of an address and where appropriate the geographic location of an address.

This serious concern has since turned into a reality with the Minister's announcement on the 8th of October 2013 that Cabinet had agreed to the rollout of the unique seven digit character code to every letter box in the State by 2015. A consortium headed by Capita Ireland has been engaged[9] to develop, implement and operate the new postcode and…

" Under the new system, Ireland will be the first country in the world to have a public database of unique identifiers for all properties that will assist citizens, public bodies and business to locate every individual household in the State. "

This Office is unaware as to how this Consortium in conjunction with the Department will ensure that the Individual citizen's fundamental right to data protection (and Privacy) will be safeguarded into the future by the use of this postcode. In particular whether these safeguards will be statutorily ringfenced such as proposed to be done in relation to unique seven digit medical identifiers as proposed by the Individual Health Identifier Bill 2013 or how both public and private bodies will be in compliance with the Data Protection Act, in the use of this Postcode. We have made enquires from the Department to this effect and will continue to do so pending complete clarification as to the manner in which the postcode system will operate in compliance with the Data Protection Acts.

[9] See S.66 subsection (2) of 2011 Act

Commission for Energy Regulation (CER) - Smart Metering

Continuing from previous engagement in 2012, we have worked with the Commission for Energy Regulation on issues related to data protection in the proposed rollout of Smart Meters to Irish households. The Smart Metering project has not yet reached implementation stages, but has already started taking the views of stakeholders. This includes consultation with the energy network providers and the energy supply companies. We have outlined concerns in relation to data protection to do with the proposed frequency of meter reading; the basis for it; the type and nature of personal data that is collected by smart meters; the transparency of information available to individuals; and the range of personal data "controls" available to them. We also proposed that a Privacy Impact Assessment be carried out to involve the stakeholders and individuals in order to directly identify and assess the concerns people have; the tools, techniques and limitations that can be used to minimise any impact or risk to personal data; and the means to measure the success of those tools and techniques. We welcomed the inclusion of a data protection team into the CER's organisation that is working to bring this project and the associated infrastructure changes to fruition in Ireland in the coming years.

CONSULTATION ON NEW LEGISLATION

The Office provided legal assistance and guidance on data protection issues in relation to many pieces of legislation either proposed or soon to be implemented. The following are some of the Bills / Acts that we provided advice on:-

1. The Credit Reporting Bill 2012

We were consulted by the Department of Finance on the provisions contained in this Bill and the data protection compliance issues. Once the Bill has been enacted this Office will engage with the Central Bank of Ireland to draft Regulations that should complement the data protection safeguards. It is with disappointment that we note the use of PPSN as a personal identifier but we understand the reasoning that the CBI

requires credit institutions to collect the PPSN to ensure that the information provided to the Register is accurate and relates solely to the individual concerned. One key protection in the Bill is that the Data Protection Act is to apply in full to the provisions of the Credit Reporting Bill and that the CBI will have to notify this Office of any systemic problems in relation to obtaining, keeping, processing, or use of information held on the Register. Another unique feature of the Bill is that business entities that have a turnover not greater than €3 million will be covered by Data Protection.

2. The Health Identifier Bill 2013

This Bill when enacted will create a seven digit number similar to the PPSN which is to be used to identify every individual availing of a health service. The number will be associated with medical service providers and the actual service provided. All registered medical service providers will have an identifying number assigned to them also. The purpose is to ensure that there is improved patient safety and a reduction in adverse events due to misidentification of patient care across organisational boundaries and the public and private health sectors. No clinical data can be part of the identifying particulars contained in the IHI dataset. This Office assisted the Department of Health with comments on the draft provisions and any issue regarding the processing of personal data. One unique provision of the Bill is that the IHI number will be defined as being personal data and will apply to deceased persons. We shall continue to assist the Department on the rollout of the Act once it has been enacted and commenced as expected in 2014.

3. Water Services Act 2013

This Act provides for the establishment of "Irish Water" who, in conjunction with Bord Gais Eireann, are the metering authority with responsibility for the installation of water meters throughout Ireland. We were consulted by and advised both

companies both prior to and after the commencement of the Act. This concerned what the process would be to obtain verification of personal information, such as name and address of householder from relevant parties as set out in Section 26 of the Act, which could be done in practice through contractual arrangements which provide appropriate safeguards and security for the transfer of large datasets. We will continue to engage with Irish Water in 2014 on any data protection issues that arise.

4. Sport Ireland Bill 2013

We were requested by the Department of Sport to give our observations on the proposed Bill which will establish "Sport Ireland". One issue that arises relates to this new organisation being the National Anti Doping Authority for Ireland and the complex international agreements in place with organisations such as WADA who manage the World Anti Doping Code. Athletes who compete in international competition are required to be monitored and provide medical sampling and other personal data. A concern has been raised at EU level (Article 29 Data Protection Working Party) about the transfer of medical and other personal data of athletes to countries that may not have sufficient safeguards and controls in place for the proper security and protection of this sensitive information. This consultation with the Department is ongoing and will continue into 2014.

5. Criminal Justice (Forensic Evidence and DNA database System) Bill 2013

There have been many submissions made by legal and human rights organisations about the profound effects that this Bill will have on the Constitutional and Human Rights of the Individual. The Bill itself contains many built in protections to balance the effects of the Bill with the rights of the Individual. One pertinent safeguard from this Office's point of view will be that a representative from this Office will be part of the oversight committee who's independent function will be to oversee the management and operation of the DNA database system for the purpose of maintaining the security and integrity of the system and to ensure that the (safeguard) provisions of the Act are complied with.

6. Personal Insolvency Act 2012

Upon the creation of the Insolvency Service of Ireland we met with the new Director and his staff and provided advice and assistance on the practical implications of implementing some of the provisions of the Act.

Binding Corporate Rules (BCR)

The EU Data Protection Directive and the Data Protection Acts impose conditions on the transfer of personal data to countries outside of the EEA that are not considered to provide an "adequate" level of data protection. Organisations that transfer personal data outside of the EEA must do so in accordance with the provisions of Section 11 of the Data Protection Acts. To facilitate multinational companies with operations in many countries, the Article 29 Working Party developed an alternative system of "Binding Corporate Rules" (BCR). BCR allow the composite legal entities of a corporation to jointly sign up to common data processing standards that are compatible with EU data protection law and thereby receive approval for their intra-group data transfers.

In 2013, the process of approving processor BCR also commenced. BCR for Processors are meant to be a tool which would help frame international transfers of personal data that are originally processed by a Processor on behalf of an EU Controller and under its instructions, and that are sub-processed within the Processor's organisation.

In order to secure approval for BCR, a company must choose a lead data protection authority to coordinate securing approval from other relevant data protection authorities. The lead authority must also, as part of this process, formally approve the BCR with the help of two co-reviewer data protection authorities. In 2013 this Office acted as co-reviewer on two BCR applications. We also received one application to act as lead authority on a processor BCR and work on this application is ongoing.

Codes of Practice

Section 13 of the Act provides that the Data Protection Commissioner

"shall encourage trade associations and other bodies representing categories of data controllers to prepare codes of practice to be complied with by those categories in dealing with personal data."

These Codes of Practice are designed to give operational meaning to the principles of data protection set out in European and National law. In 2013 this Office approved a Code of Practice for the Insurance Sector under section 13(2) of the Acts. This Office worked with Insurance Ireland on this code for a number of years before reaching completion in June 2013. On approving this code the Commissioner stated:

"I am confident that the Code will make a significant contribution to improving knowledge and understanding of data protection within the Insurance sector. I intend to continue to work closely with Insurance Ireland to ensure that the guidance set out in the Code is followed in daily practice."

EU & International Responsibilities

New EU Data Protection Laws

In January 2012, the European Commission published its proposals for a strengthening of EU data protection law, reflecting the enhanced status given to data protection by the Lisbon Treaty. The Commission proposals provided for a directly-applicable Regulation imposing stricter obligations on data controllers and processors and enhanced rights for data subjects. The Commission proposed a separate Directive covering the area of criminal justice.

The proposals were the subject of much discussion in the course of the year, particularly by the co-legislators, the European Parliament and the Council of Ministers. The key European Parliament Committee (LIBE) approved a revised text of both proposals in October. While significant progress was made in the Council in the first half of the year under the Irish Presidency, an agreed position could not be achieved by end-year. It therefore seemed unlikely that the proposals could be signed into law in 2014.

The proposals, if passed into law, will involve increased responsibilities for our Office under the so-called "one-stop-shop" arrangement for oversight of multinational companies providing services to EU users from an Irish base.

Article 29 Working Party

The Article 29 Working Party acts as an adviser to the European Commission on data protection issues. It also promotes a uniform application of EU data protection law throughout the European Economic Area.

In the course of 2013, the Working Party continued to give close attention to issues relevant to the future EU data protection regime. It also produced Opinions on Smart Grids and Smart Meters; "Cookies"; Reuse of Public Sector Information; Smart Borders; Binding Corporate Rules; Apps on Smart Devices; and the Purpose Limitation Principle.

The Office continued to be represented at subgroup level at the subgroup on Borders, Travel and Law Enforcement and the Technology subgroup.

Further information on the Working Party is available on its website.

Data Protection in EU Specialised Bodies

The Office continued to be represented at meetings of the data protection bodies overseeing activities in specialised EU bodies. These are the EUROPOL Joint Supervisory Body (which reviews the activities of EUROPOL to make sure that its use of personal information does not violate individual privacy rights), the Customs Joint Supervisory Authority and the EUROJUST Joint Supervisory Body (which ensures that cross-border cooperation between EU judicial and prosecution authorities respects data protection rights).

International Activities

We were represented and spoke by invitation at the 34th International Conference of Data Protection and Privacy Commissioners hosted by our colleagues in Poland.

We continued to follow the useful work being done in the OECD, especially in the area of cross-border enforcement of data protection.

We continued to assist our colleagues, in the EU and elsewhere, where they were dealing with complaints in relation to Irish-based organisations or seeking information on our data protection practices. We also participated in a number of EU-funded outreach activities towards EU candidate countries.

We further developed our cooperation with the Federal Trade Commission of the United States – a key privacy enforcement authority – especially through the signing of a Memorandum of Understanding. We also signed an updated Memorandum of Understanding with the Office of the Privacy Commissioner of Canada. These MOUs facilitate the type of practical cooperation that is becoming increasingly important for the effective oversight of global companies operating on the Internet.

We also continued our involvement with the Global Privacy Enforcement Network (GPEN), the International Association of Privacy Professionals (IAPP) and the Commission for the Control of INTERPOL's Files (CCF).

Administration

Running Costs

The costs of running the Office in 2013 were as follows:

	2013 (€)
Overall running costs	1,960,999
Receipts	660,290

A fuller account of income and expenditure in 2013 is provided in Appendix 3.

Part 2 – Case Studies

Case Study 1: "Feet-On-The-Street" Marketing by Electric Ireland is Subject of Complaint

The Office received a complaint from an individual concerning a visit by an Electric Ireland sales representative to his home. The complainant explained that a sales representative called to his door, displayed his identity card and stated that he was calling with a new offer on behalf of ESB Electric Ireland to addresses of former ESB customers. The sales representative then informed the complainant that he was aware that he was a previous customer of ESB. He proceeded to produce a document which listed the complainant's house name, his address, the date on which he switched his account from ESB and the MPRN (Meter Point Reference Number) at the house. The sales representative went on to say that, as the complainant had switched from ESB in 2009, he was now on his current electricity supplier's highest rate and, therefore, he could switch back to avail of new rates with Electric Ireland which would be considerably cheaper than his current rates.

On foot of this complaint, we commenced an investigation by writing to Electric Ireland. We questioned why the sales representative was in possession of information relating to a former customer, in particular the MPRN and the date of leaving ESB, and why Electric Ireland was retaining this data.

In response, Electric Ireland confirmed that the sales representative was in possession of three specific pieces of information: MPRN, MPRN address/location and the date of the last registration of the MPRN against an Electric Ireland account. It said that the sales representative did not have the complainant's name or any other personal information. In relation to MPRN, Electric Ireland stated that this information is available to all licensed electricity suppliers in the Irish electricity market. It said that it was using this information for the exact purpose of identifying a service delivery

point where a customer may have a network connection agreement and where metering may be installed. In relation to data retention, Electric Ireland referred to various legislative requirements in the VAT code and in a statutory instrument (SI 385 of 2008).

In response we informed Electric Ireland that the retention of personal data in those particular contexts were for purposes set down by the Revenue Commissioners and that it did not give data controllers any entitlement to use the retained data for its own other purposes, such as for marketing. We pointed out that there was no legitimate basis under the Data Protection Acts for Electric Ireland's marketing department to access ex-customer personal data for the purposes of win-back campaigns unless the ex-customer consented to marketing contact prior to the termination of their contract. We made it clear that to supply sales representatives with details of the date of the last registration of the MPRN against an Electric Ireland account amounts to unlawful further processing of personal data. We told Electric Ireland that there was no legal basis for it to access MPRN data for the purposes of marketing to non-customers. For that reason, we advised Electric Ireland that MPRN data should not be accessed for marketing purposes or supplied to "Feet-On-The-Street" agents. We asked it to commit to cease using MPRN data for marketing purposes.

In response, Electric Ireland committed to the removal of MPRN data from all “Feet On The Street” marketing lists with immediate effect. It also indicated that it was retracting all marketing lists containing MPRN data forthwith and it undertook to provide immediate re-training to staff. For completeness, within a short period we sent an inspection team to Electric Ireland to examine the implementation of our recommendations. This allowed us to examine the company's marketing campaign procedures at first hand. The inspection team comprised staff of this Office and of the Commission for Energy Regulation. The inspectors were satisfied that Electric Ireland had ceased using MPRN data in marketing campaigns. In addition, the inspectors noted that, if a customer decides to move from Electric Ireland to another service provider, the departing customer’s details are subsequently deleted from the company's marketing database.

This case is of particular importance to all service providers in the electricity and other utility sectors. Win-back campaigns targeted at former customers are common place and the data controllers concerned are often tempted to delve into personal data retained for particular statutory requirements in order to create or enhance their marketing lists. We urge such data controllers to tread carefully in this space as, without the prior marketing consent of the former customers concerned, there is no legal basis to process marketing lists using such retained personal data.

Case Study 2: County Council Causes Breach by Outsourcing Data Processing to Third Party

The Office received a complaint against Westmeath County Council regarding the outsourcing of customer details relating to the Council's domestic refuse collection service. The complaint alleged that customer details were unlawfully outsourced by Westmeath County Council to a third party for the purpose of notifying householders of the sale of the Council's waste collection service.

In response to our investigation of the complaint, Westmeath County Council stated that it had tendered for the provision of a refuse collection service in 2009, having decided to outsource this service which was part of the Council's general service provision. The successful bidder was provided with a list of names and addresses of the property owners availing of the service at that time. We asked Westmeath County Council to inform us of the name of the entity to whom the printing and issuing of the letters which notified householders of the sale of the waste collection service had been outsourced. We also requested details of any contract in place between Westmeath County Council and the entity concerned. Westmeath County Council confirmed that a local printing company in Mullingar had successfully tendered for the printing and postage of the letters and that it had been supplied with a copy of the Council's waste collection service database containing approximately 15,000 names. It also informed us that there was no formal contract in place between the Council and the printing company governing the use of the database by the printing company.

The printing company subsequently confirmed to Westmeath County Council that it had received the database and had used it only for the purpose of notifying persons/households of the revised refuse collection arrangements. In addition, the printing company confirmed that this database was never otherwise used or passed to a third party but was destroyed on completion of the printing job.

The complainant in this case sought a formal decision on his complaint.
The Commissioner formed the opinion that Westmeath County Council contravened

Section 2C(3) of the Data Protection Acts by failing to have a contract in place with the printing company concerned for the processing of personal information. This contravention occurred when Westmeath County Council outsourced to a third party the printing and distribution of letters and provided it with a copy of its customer database containing the complainant's personal data for this purpose, without having a contract in place for the processing of the personal data.

The outsourcing of data processing to third parties for the purposes of data processing is frequently a matter of concern to data subjects who contact this Office. The data protection framework makes specific provision for the engagement by data controllers of data processors to carry out data processing functions on their behalf. This provision requires the data controller to put in place a contract in writing or in equivalent form between it and the data processor concerned. This contract legitimises the passing of personal data from the data controller to the data processor for data processing purposes. Obviously, we would expect contracts to contain some clause or clauses which bind the data processor to compliance with the Data Protection Acts in terms of the handling, storage, security and processing of the personal data concerned. The passing of personal data by a data controller to a third party in the absence of such a contract is unlawful as it effectively amounts to a disclosure of personal data to a third party without a legal basis. As can be seen in the above case, it was solely the absence of a contract which led to the breach of the Data Protection Acts which took place.

Case Study 3: Government Department admits inappropriate access to records by an official.

The Office received a complaint in May 2012 against the Department of Social Protection. The complainant alleged that there had been unauthorised access within the Department to his records by a departmental employee.

We commenced an investigation of the matter by writing to the Department of Social Protection outlining the details of the complaint. In response, the Department of Social Protection confirmed that the complainant had previously requested from the Department of Social Protection, by way of an access request, a 'log of accesses' made to his social welfare records. It stated that, during follow-up contact with the complainant, it became clear that the complainant was concerned that a particular individual employed by the Department, his ex-wife, may have inappropriately accessed his details.

The Department of Social Protection subsequently informed us that a full investigation of the matter had been undertaken. The Department indicated that, during the course of this investigation, a member of staff admitted to accessing the complainant's records without having a legitimate business reason for doing so. It said that, as a consequence, the matter had been referred to the HR Division for possible action under the Civil Service Disciplinary Code. The Department apologised to the complainant for any distress that the breach may have caused him. It said that the Department takes its responsibility as a data controller very seriously and that it makes every effort to ensure that personal data is safeguarded at all times.

We sought specific details from the Department regarding when and how often the unauthorised accesses had occurred so that the extent of the breach could be determined. In response the Department gave us details of the dates and times of each unauthorised access. There were twelve instances of unauthorised access of the complainant's records between February 2004 and July 2009 by a member of staff who did not have a legitimate business reason to do so.

A formal decision on the complaint was requested by the solicitor acting for the complainant.

The Commissioner's decision, which issued in February 2013, found that the complainant's personal data was further processed by the Department of Social Protection in contravention of Section 2(1)(c)(ii) of the Data Protection Acts, 1988 & 2003 on twelve separate occasions. These contraventions occurred when the complainant's records, which were held on the Department's customer information database, were accessed by an employee of the Department for a purpose unrelated to that for which the data was obtained.

Once again this case highlights the unacceptable practice by some individuals of snooping through official records for personal reasons unconnected with their official duties. Varying degrees of personal information relating to every citizen in the State is held on databases within Government Departments and officials who have access to this information to conduct their official duties are entrusted to access and use that information in accordance with the requirements of their functions. Straying beyond the boundaries of their official duties in terms of accessing personal records amounts to unlawful activity by the individuals concerned. For that reason, it is critical that data controllers, such as a Government Department in this case, have robust disciplinary policies in place to deal with any breaches. Taking no action against individuals caught engaging in such activity is not acceptable. Instead, it should be clear to all users that there are serious negative consequences for unauthorised access to personal information for unofficial purposes. Furthermore, as this case demonstrates, it is vital that data controllers have an audit trail in place on computer systems to capture both 'read-only' and 'edit' accesses to official records. Obviously the monitoring of such audit trails and follow-up action are crucial elements in ensuring the effective protection of records which are stored on a data controller's computer systems.

Case Study 4: Excessive data requested by a management company

In April 2013 we received a complaint from a tenant of an apartment complex who stated that the management company of the complex was in the process of introducing a new key pad access system to resolve serious security issues in the complex. The complainant stated that he considered that the management company was requesting excessive information in order for tenants to have access to this new system. The complainant supplied us with a copy of a letter which had been issued by the management company. The information sought in order to access the new system included a copy of passport/driving licence, PPS Number, emergency contact details, vehicle details, employment details and a copy of a current lease/tenancy agreement.

We contacted the management company asking that it outline the legal basis for the requesting of this level of personal information. In response, the management company explained that the complex was fully tenanted with no owner occupiers. It asserted that the request for the information was based on the fact that it had found in the past that information supplied by landlords did not always tally with who was actually living in the complex. We stressed to the company that any personal information sought should be adequate, relevant and not excessive in relation to the purpose for which it was obtained and held. We said that we considered that the level of personal information being sought was excessive in relation to the introduction of a new access system to an apartment complex.

In response to our intervention the management company drafted a revised letter for issue to the tenants of the complex and it submitted it to us for consideration. This letter limited the personal data sought to emergency contact details, vehicle details and a copy of a current lease/tenancy agreement.

We informed the management company that we considered the information now requested to be fair and reasonable for the purpose for which it was sought. However, we informed it that, as a data controller, it has obligations in relation to the processing of the information such as ensuring that all personal information collected be kept safe and secure, not be disclosed to a third party and that arrangements be put in place to have all personal data deleted when a tenant moved out of the complex. In addition,

we stated that tenants should be informed that they could redact the rent amount from the copy of the lease/tenancy agreement submitted to the management company. The management company confirmed that it would comply with these obligations.

The complainant subsequently notified us that the management company had issued the revised letter to tenants. As a result of this complaint to the Office, the management company significantly reduced the amount of personal information it required from tenants in order to register for the new access system.

The Data Protection Acts require that an appropriate balance be struck between the privacy considerations of the service user, in this case the apartment tenants, and the legitimate interests of a data controller to protect its business, in this case the management company. We considered that the revised letter issued to tenants by the management company struck the appropriate balance in this case.

Case Study 5: No breach found in data disclosure case.

In June 2012 we received a complaint from a data subject who stated that, while in the employment of a beauty salon, she made a telephone enquiry to a beauty products supply company as she was considering starting her own business and carrying that company's products. The supply company also supplied products to the beauty salon where the complainant worked. The complainant informed us that, following this phone call, she returned to work some days later and was told by her employer that she was being laid off as her employer had received a telephone call from the beauty product's supply company which revealed that she was considering setting up her own business.

We commenced our investigation by writing to the beauty products supply company asking it to outline the basis for allegedly disclosing the contents of the telephone conversation concerned. In reply the company said that it felt obliged to notify the owner of the beauty salon of the phone call. It said that it was concerned that this information would be in the beauty salon's interest as it thought that the setting up of a new business would be business competition for the beauty salon, the complainant's employer.

Our approach to complaints, as provided under the Acts, is to try to reach an amicable resolution to the matter which is the subject of the complaint. In this regard the beauty products supply company offered the complainant €1,000 in an effort to amicably resolve her complaint. However, the complainant refused this offer and she sought a formal decision on her complaint.

The issue that arose for consideration in the decision was whether the Data Protection Acts were breached when the beauty product's supply company disclosed the contents of a telephone conversation about the complainant to her then employer, the beauty salon.

One of the conditions under which the processing of personal data may be carried out is where the processing is necessary for the legitimate interests of the data controller (in this case the beauty products supply company) except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject.

In his decision, the Commissioner considered that, when the beauty products supply company contacted the complainant's then employer and informed it that the complainant had been in contact with it in relation to setting up her own beauty salon and carrying their products, it was reasonable for the beauty products supply company to consider that the disclosure of that information was in its legitimate interests of maintaining an ongoing commercial relationship with the beauty salon. As the complainant had indicated to the beauty products supply company that the reason for the enquiry about its products was that she was considering setting up her own business in a different location, which would have involved her leaving the beauty salon, the Commissioner did not consider that the disclosure was unwarranted by reason of prejudice to her fundamental rights and freedoms or legitimate interests. In the circumstances, the Commissioner was unable to form the opinion that the Data Protection Acts were breached in this case.

Case Study 6: Doctor discloses sensitive personal data to insurance company without consent

This Office received a complaint from a solicitor acting on behalf of a data subject concerning the alleged further processing of the complainant's personal data contained in medical records held by her General Practitioner (GP). It was alleged that medical records relating to the complainant were released to an insurance company by her GP, following a request made to the GP. The complaint stated that the GP had received a request from an insurance company seeking the complainant's medical records relating to a knee injury she had suffered. It was alleged that, in replying to this request, the GP not only released data relevant to the knee injury, but he also disclosed other sensitive medical information - including cervical smear test results, a colposcopy, correspondence regarding lesions and records relating to Carpel Tunnel Syndrome, none of which were related to the knee injury.

We wrote to the GP and we asked that he provide an explanation as to what had occurred in this case. He responded stating that an insurance company had requested relevant information with respect to the patient concerned and her knee injury. He informed us that the request received stated that it 'required copies of clinical consultations / surgery notes, investigations and associated results, treatments, referrals, outpatient appointments and repeat prescriptions from 18.2.2009 to the present date'. He stated that, inadvertently, copies of the patient's records were supplied to the insurance company with some details which were not relevant to her knee injury and that this was obviously an oversight. He stated that he was deeply sorry that he had caused any distress or upset to his patient whom he had known for thirty five years. The GP stated that the complainant knew that he always endeavoured to keep a high standard in the practice and that she should understand his disappointment that the system used in releasing this information fell below the standard expected by the complainant and himself. He further stated that he hoped that she would accept his unreserved apology for the inadvertent disclosure of her records to the insurance company and that he completely understood how upset and

disappointed she must be. He said that since this unpleasant and unfortunate error he had overhauled his practice procedures.

We wrote to the solicitor for the complainant outlining the GP's response and also conveying the GP's apologies. We stated that this Office's approach to complaints is to try to seek an amicable resolution to the matter which is the subject of the complaint and we asked if his client would like to try to reach an amicable resolution of the complaint. They responded stating that their client wished for a formal decision of the Commissioner on the matter.

In considering this case, the key issue from a data protection perspective was the issue of consent. It was noted from the material provided that the complainant had completed and signed an insurance claim form which contained the following consent clause: *"I authorise Financial Insurance Company Limited (the Underwriters) to make any enquiries and get any information they consider relevant from my doctor, employers or elsewhere. I understand that I must provide evidence to Financial Insurance Company Limited to prove my claim."* On the same claim form, the complainant supplied details of her accident and explained, as follows, why it prevented her from working: *"Left knee injury. Tore Ligaments. Recovery Time Unknown. Waiting for Knee Surgery. On Waiting List."*

The insurance company concerned had sought the complainant's medical records, supplied the relevant consent form and used the following terms in its request to the GP: *"Can you please provide us with copies of the claimant's medical records relevant to this claim. This includes all records relating to the medical conditions and associated symptoms which are the subject of this claim."*

It was clear from the insurance company's request for medical records that it sought medical records relevant to the claim only. As the claim related to the complainant's knee injury, the medical records sought related to that injury and the request did not extend beyond that. Equally, the complainant's consent authorised the insurance company to make enquiries and to get any information considered relevant from her doctor and others. The consent was clearly limited to relevant information and it could not be interpreted as extending to all medical records held by the GP.

This Office issued a decision on this complaint which stated that the Commissioner was of the opinion, following the investigation of this complaint, that Section 2(1)(c)(ii)of the Data Protection Acts, 1988 & 2003 had been contravened by the GP by the further processing of the complainant's sensitive personal data in the form of medical records unrelated to her knee injury. The contravention occurred when the GP, in responding to a request from an insurance company, disclosed to that insurance company certain medical records of the complainant without her consent.

Case Study 7: Customer information disclosed by phone retailer

This Office received a complaint from a solicitor acting on behalf of a data subject alleging a data breach which occurred at the Carphone Warehouse following the theft of the data subject's mobile phone. It stated that the data subject's mobile phone had been stolen while she was out shopping and that the incident had been immediately notified to An Garda Síochána, who traced the mobile phone to a park in the town where it had been stolen. However, the mobile phone had not been recovered at that time. The complaint stated that, on the following day, two individuals arrived at the data subject's isolated family home with the stolen mobile phone and they sought a reward for finding it. The complaint stated that the data subject handed over €50 and the stolen mobile phone was returned to her albeit damaged in what seemed to be an effort to extract the SIM card.

The complaint further stated that, shortly after this incident, the data subject contacted her local branch of Carphone Warehouse and was informed that two people had called there claiming that they had found the stolen mobile phone and that they were looking for contact details of the owner in order to return it. The complaint alleged that the Carphone Warehouse employee gave these two people the owner's name and address. The complaint stated that the data subject was in contact with both local and regional management of the Carphone Warehouse but she considered that they failed to grasp the seriousness of the situation. She was offered a new mobile phone plus a written apology from Carphone Warehouse but she declined to accept this offer.

We commenced our investigation into this matter by contacting Carphone Warehouse and outlining the details of the complaint. We asked it to explain how the complainant's personal data was allegedly disclosed in the manner outlined in the complaint.

We received a reply from Carphone Warehouse which stated that, on the evening concerned, two people presented to one of its stores with a handset which they claimed their daughter had found and which they were seeking to return to the rightful owner. The staff member in the store at the time was a trainee who initially recommended that they present the handset to the local Garda Station. However, the

people said that they wanted to be sure that the person received their handset. Carphone Warehouse stated that the staff member then disclosed the owner's address so that the handset could be returned, mistakenly thinking that he was assisting the customer. It acknowledged that this was an obvious and serious breach of its policies and procedures. It stated that it conducted a full investigation, including a formal interview with the staff member and identified that this was very poor judgement but in no way malicious as the staff member had nothing to gain personally from this action. It acknowledged that this in no way took from the severity of the breach but was factored into its internal actions for the staff member in question. Carphone Warehouse stated that it would again like to express its sincerest apologies to the data subject and it also offered to replace the customer's handset and provide an additional payment of €100.

Following on from this correspondence, we wrote to the solicitor for the data subject stating that it was the view of this Office that Carphone Warehouse had contravened the Data Protection Acts in terms of how the data subject's details were disclosed by its employee. We also stated that, as provided for under the Acts, it was our aim to amicably resolve complaints and to this end we stated that Carphone Warehouse had offered its sincere apologies, offered to replace the complainant's mobile phone with a new one at a cost of €500 and offered a gesture of €100.

In response, we were informed that the data subject was not willing to accept the offer of an amicable resolution to her complaint made by Carphone Warehouse and a formal decision was required.

A decision issued on this complaint which stated that the Commissioner was of the opinion that, following the investigation of the complaint, that Carphone Warehouse contravened Section 2(1)(c)(ii) of the Data Protection Acts 1988 & 2003 by disclosing the data's subject personal data to a third party without her knowledge or consent. This contravention occurred when the personal data of the complainant was disclosed by Carphone Warehouse to a third party or parties without her knowledge or consent.

A key principle of data protection is that personal data should be kept safe and secure and not be disclosed to unauthorised third parties. The actions of the Carphone Waterhouse employee in this case in disclosing the data subject's address to strangers resulted in considerable distress for the data subject. Despite initially telling the individuals who were in possession of the mobile phone to present it to An Garda Síochána, which was the correct procedure for such cases, he then proceeded to disclose the data subject's personal information to third parties. Regardless of the fact that the employee concerned was a trainee, this disclosure should not have happened. Data controllers should be vigilant at all times to ensure that appropriate procedures are in place to prevent disclosure of personal data to third parties and that all employees abide by them.

Case Study 8: CCTV images of staff member unlawfully transmitted to third parties

This Office received a complaint from a solicitor acting on behalf of a data subject concerning the alleged further processing of the complainant's personal data, as contained in CCTV footage captured in the complainant's place of work, a Spar store. It was indicated that, following an incident in the Spar store which resulted in the complainant falling, CCTV footage of the incident was accessed, copied to a mobile phone by another staff member in the company of a manager and circulated to third parties. It was contended that this action constituted a breach of Section 2(1)(c)(ii) of the Data Protection Acts as the purpose for the use of CCTV within the shop was for security purposes. The complainant provided us with a CD of the CCTV footage concerned which appeared to show a shop attendant tripping and falling behind a shop counter.

We commenced an investigation of the matter by writing to Spar outlining the details of the complaint. We received a response from Spar which stated, among other things, that: "This behaviour is regrettable and completely in contravention of the ethos of the business. The policy of this store has always been, and is still, that access to our CCTV equipment is only available to the management team and members of the Gardaí. In this instance, members of the management team, ……. were involved and this is unforgivable." We were also informed that the members of the management team involved were no longer employed by the Spar store concerned.

Having regard to the complaint and the response received, we informed Spar that we were of the opinion that Section 2 of the Data Protection Acts had been contravened by the processing and disclosure of the complainant's images from the CCTV system in Spar and we requested proposals for an amicable resolution of the complaint.

Solicitors acting on behalf of Spar wrote to us stating that its client was concerned and apologetic that the matter had arisen. They informed us that the members of staff responsible for the release of the CCTV data were severely reprimanded as they were in serious breach of shop policy. They also informed us that their client was interested

in amicably resolving this complaint by acknowledging the error and conveying apologies to the complainant in writing. However, the complainant's solicitor sought a formal decision on this complaint.

The decision which issued on this complaint stated that the Data Protection Commissioner was satisfied that the complainant's personal data was further processed by Spar in contravention of Section 2(1)(c)(ii) of the Data Protection Acts 1988 & 2003. This contravention occurred when the complainant's personal data (CCTV footage) was accessed, copied and circulated by staff of Spar for a purpose unrelated to those purposes for which the data was obtained.

The misuse of CCTV in this instance clearly contravened the Data Protection Acts. Modern technology provides an easy means for recorded footage to be accessed and transmitted to a wide audience in a very short time, often causing considerable distress to individuals whose images appear in the footage. Data controllers should be constantly vigilant to ensure that CCTV footage of individuals is processed only for its intended purpose, is restricted from access by staff who have no business need to access it, and that all managerial staff handle such footage with the level of care that is expected for the processing of personal data generally.

Case Study 9: Data controller legitimately uses CCTV in disciplinary proceedings.

This Office received a complaint which stated that a supermarket instructed a third party to remove a CCTV hard-drive, containing CCTV footage of the complainant's image, from the store where the complainant worked as store manager and that no member of the supermarket staff accompanied this third party contractor during the removal. The complainant alleged that the supermarket viewed three weeks of CCTV footage which contained the complainant's image and used this CCTV footage to ground a disciplinary hearing against the complainant. The complaint stated that at no point was the complainant consulted in relation to the removal, viewing or processing of the CCTV footage.

We commenced an investigation of the matter by writing to the supermarket outlining the details of the complaint. In response, the supermarket informed us that it was contacted by an external third party alleging irregularities in the cash management process in its store. An investigation into these irregularities was initiated and CCTV footage was secured in that process in line with the company's purpose for CCTV, namely to "protect against inventory loss by criminal actions." It said that the CCTV recorder was removed by an authorised contractor, who did not carry out any maintenance which requires supervision, but solely removed the unit and transferred it to its regional distribution centre where it was securely kept in a locked room and footage was only reviewed by employees tasked with the investigation into the allegation. It informed us that the contents of the CCTV footage was explained verbally to the complainant to allow him to explain the irregularities in the cash handling process. The supermarket told us that, as a retail business which is handling large sums of monies on a daily basis, it felt that its actions were guided by a legitimate interest to protect its vested rights and property.

We sought information from the supermarket regarding the 'external third party' who retrieved the CCTV footage from the store, and whether the CCTV footage in question demonstrated an "inventory loss by criminal actions." It informed us that the third party who retrieved the CCTV footage was its contracted CCTV service

provider. It said that, in this incident, the contractor did not carry out any processing, but merely took the CCTV recorder from the store to the regional distribution centre. It further stated that the CCTV footage showed actions that were questionable, but that no conclusions were drawn from the footage as to whether the actions were of a criminal nature or a performance and conduct issue. It was satisfied from the complainant's explanations that the actions were not of a sinister nature, but instead constituted a total disregard for internal cash management procedures. It said that the complainant was subsequently disciplined for this matter.

We conveyed the explanation provided by the supermarket to the solicitor acting for the data subject. In response it was argued that the employer had already established that there was no cash missing by inspecting the safe and accordingly, there was no need to then review CCTV footage. It was further stated that the amount of CCTV footage viewed was excessive and disproportionate as the irregularities in relation to cash handling took place over a seven day period, but three weeks of CCTV footage was examined by the supermarket during the course of its investigation into the cash handling irregularities.

In response to this, the supermarket stated that the irregularities brought to its attention by the external third party were of such a complex and serious nature that it was not possible to fully investigate the matter by conducting a safe count alone. It further stated that it acted reasonably and proportionately and in compliance with data protection legislation when investigating the irregularities in the cash management process. We wrote to the supermarket seeking further specific information regarding the irregularities reported to it and how the investigation of same progressed. It informed us that it was notified by an external third party about irregularities in the cash management process. Two issues were identified, both of which involved substantial sums of money. The supermarket commenced its investigation of the matter as soon as the issues were identified. It stated that: "In order to preserve the CCTV footage for the investigation and to protect it from being overwritten, the DVR unit had to be removed by the contractors. CCTV footage from the 3rd January to 23rd January was viewed by the investigators, due to the fact that it was impossible to investigate the irregularities which took place on the 9th and the 16th of January in

isolation, and given that the entire cash management for that period was relevant for the investigation." It was further stated that the complainant was afforded the opportunity to view the entire footage in line with fair HR policies and proceedings.

The complainant sought a formal decision of the Data Protection Commissioner on his complaint. The key issue that arose for consideration under the Data Protection Acts was whether the supermarket acted in accordance with the requirements of the Acts when it processed CCTV footage which contained images of the complainant. The supermarket viewed CCTV footage for the period of 3 January 2012 to 23 January 2012. This footage was viewed as part of an investigation to determine whether any fraudulent or criminal activities had taken place following the reporting of irregularities to the supermarket by a third party and an alert being raised by its own internal processes. Section 2A(1)(d) of the Acts provide that a data controller shall not process personal data unless "*the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject."* The Data Protection Commissioner considered that, when the supermarket viewed the CCTV footage for the period, it did so in the pursuit of its own legitimate interests. The Commissioner did not consider that the processing of personal data in this case was unwarranted by reason of prejudice to the fundamental rights and freedoms or legitimate interests of the data subject. Following the investigation of the complaint against the supermarket regarding its processing of the complainant's personal data in the form of CCTV footage, and having regard to the legitimate interests of the employer in this case, the Commissioner was unable to conclude that a contravention of the Data Protection Acts took place in this instance.

This Office is receiving an increasing number of complaints concerning the use of CCTV in a range of environments. Many are against employers and the alleged use by them of CCTV to monitor employees as they go about their workplace duties. The use of CCTV in employment situations must be proportionate and transparent and the default position is that CCTV should only be used for stated valid purposes such as

security. CCTV footage should not be used as a tool for staff performance monitoring. Having examined the issues raised in this complaint, however, it was considered that the data controller in this instance presented this Office with a genuine security reason for processing the CCTV images of the complainant and accordingly, the processing could not be deemed to contravene the Data Protection Acts.

Case Study 10: Breaches by hotel in use of photographs of employees in dismissal cases

This Office received separate complaints from two former employees of an hotel in Dublin 2 in relation to similar incidents which occurred six months apart. Both complaints concerned the alleged unfair processing of personal data by the hotel. In both cases the complainants worked as night porters, and they both faced disciplinary proceedings for allegedly sleeping on duty. In both cases, the evidence used to ground the disciplinary proceedings included photographs taken on a private mobile phone belonging to the assistant night manager, and in each case the complainant was subsequently dismissed. One of the complainants informed us that the assistant night manager who took the photograph had shown it on his mobile phone to a colleague on the evening following the incident and he contended that the manager did this in a manner which indicated that the photograph was taken as a joke.

We commenced each of the investigations by writing to the hotel outlining the details of the complaints.

In relation to the first complaint received, the hotel responded to us stating that the hotel did not request and does not condone any employee taking photographs of another employee without their knowledge. The hotel also stated that, following a full investigation into an allegation, it was found that the complainant was asleep whilst on duty and his employment with the hotel was subsequently terminated. The hotel indicated that the findings of the investigation were based primarily on the evidence taken from the assistant night manager and not the photograph. It was also indicated that the complainant had given a statement and did not deny the allegation. The hotel also confirmed that it was made aware of, and had been provided with, a copy of the photograph in question.

We sought further clarification from the hotel and it informed us that the photograph had been shared with the Director of Operations and the Human Resources Officer by the assistant night manager at the time he reported that the complainant had been sleeping on duty. The hotel stated that the mobile phone used was the personal property of the assistant night manager on duty and that no employee had been

instructed, encouraged or asked at any time to take photographs of any other employee.

We informed the hotel that, having investigated the complaint, we were of the opinion that the photograph in question was likely unfairly obtained by the hotel. We asked the hotel to confirm to this Office that the photograph had been destroyed / deleted and that they had made no use of it in its disciplinary proceedings against the employee concerned.

The hotel confirmed that the photograph had been destroyed and that the decision to dismiss the employee was not based on the photograph. However, the complainant subsequently informed my Office that an electronic version of the photograph existed and had been seen by other members of staff and that this, as well as the fact that the photograph was used as evidence against him, was recorded in the minutes of the investigative hearing.

Following an examination of the minutes of the investigative hearing which were supplied to us by the complainant, we contacted the hotel and we stated that the minutes suggested that the photograph was used by the hotel in the disciplinary process, which was contrary to what we had been previously informed. The hotel responded by saying that, while the photograph substantiated the assistant night manager's statement, it was not a determining factor in the decision to dismiss the complainant.

In relation to the second complaint, we asked the hotel to inform us if the assistant night manager had been requested to take the photograph in question by the hotel.

In response, the hotel indicated that the assistant night manager was not authorised to record images on his mobile phone and that measures had been put in place to prevent the recurrence of inappropriate use of mobile phones / mobile phone images.

Both of the complainants sought decisions on their complaints. In making his decision, the Commissioner formed the opinion that the personal data in question (in

each case a photograph of the complainant) was unfairly obtained and unfairly processed by the hotel in contravention of Section 2(1)(a) of the Data Protection Acts, 1988 & 2003. These contraventions occurred when the hotel obtained the photographs from the assistant night manager after they had been taken on his personal mobile phone, and then processed them in the course of disciplinary proceedings against each of the complainants.

Case Study 11: Incorrect application of Section 4(4A) to restrict access to personal data

We received a complaint in May 2013 from an employee of a media organisation concerning an access request he submitted to it. The complainant was concerned that he had not been provided with a copy of all of his personal data as the organisation had withheld some personal data citing Section 4(4)(A) on the basis that it considered that the data consisted of an expression of opinion given in confidence.

The focus of our investigation was to establish whether the restriction to the right of access applied by the organisation using Section 4(4)(A) of the Acts was valid in respect of the personal data which was contained in an email which was in the possession of the organisation. Section 4(4A)(a) provides as follows: *"Where personal data relating to a data subject consists of an expression of opinion about the data subject by another person, the data may be disclosed to the data subject without obtaining the consent of that person to the disclosure."* Section 4(4A)(b)(ii) provides as follows: *"Paragraph (a) of this subsection does not apply if the expression of opinion referred to in that paragraph was given in confidence or on the understanding that it could be treated as confidential.*" The organisation informed the requester that it was exempt from providing details of the data in question as the data consisted of an expression of opinion given in confidence.

As outlined in our published guidance, an opinion given in confidence on the understanding that it will be kept confidential must satisfy a high threshold of confidentiality. Simply placing the word "confidential" at the top of the page, for example, will not automatically render the data confidential. The Commissioner will look at the data and its context and will need to be satisfied that the data would not otherwise have been given but for this understanding. Supervisors and managers will not normally be able to rely on Section 4(4A) to restrict access as it is an expected part of their role to give opinions on staff which they should be capable of standing over. On the other hand, a colleague who reports a matter relating to an individual in confidence to a supervisor or manager could be expected to be protected by the confidentiality provision.

We commenced an investigation of this matter by writing to the organisation outlining the details of the complaint. We asked the organisation to provide us with a copy of the withheld personal data and details of the author of the email containing it. In order to consider the context in which the email was created, we sought details of the working relationship of the author of the email and the data subject. Having examined the email, we formed the opinion that the organisation could not rely on Section 4(4)(A) of the Acts to restrict the data subject's right of access to his personal data contained in the email. We were satisfied from our investigations that the author of the email was not a peer of the data subject but, while not considered by the organisation to be the data subject's manager, they were in a position of some authority in relation to the data subject. We were satisfied that the content of the email was supplied in the context of a position of authority. Acting on our advice, the organisation proceeded then to release the previously withheld personal data.

As this case demonstrates, the right of access to personal data may not be restricted in any widespread manner by the provisions in Section 4(4A). Even where the personal data does qualify for restriction from access, that restriction only applies to the specific opinion(s) given in confidence. In practice this means that, in the context of a full document of personal data, the data subject is entitled to access the personal data within it which is not an opinion given in confidence and the data controller may redact the part or parts which constitute the actual opinion given in confidence. As a general rule, any opinions on an individual supplied by a supervisor or manager may not be restricted under this provision.

Case Study 12: Prosecutions – Marketing Offences

GENERAL

Four Star Pizza (Ireland) Limited

This Office received a number of complaints from individuals regarding unsolicited text messages sent by Four Star Pizza (Ireland) Limited without the consent of the recipients and in some cases without the inclusion of an opt-out facility. The majority of the complainants informed us that they began to receive the unsolicited marketing text messages after placing orders in different Four Star Pizza stores. We had previously formally warned Four Star Pizza (Ireland) Limited that, if further offences were committed, the Commissioner would take prosecution action.

In response to our investigations of the complaints, Four Star Pizza (Ireland) Limited admitted that it had not obtained valid consent to send marketing text messages to the complainants. It was clear that, despite the warning issued to Four Star Pizza (Ireland) Limited, it had not put adequate procedures in place to ensure compliance with the marketing regulations. The Commissioner decided to proceed to prosecution.

At Dublin District Court on 10 June 2013, Four Star Pizza (Ireland) Limited pleaded guilty to six charges under Regulation 13(1) of SI 336 of 2011 for the sending of unsolicited marketing text messages without consent. The Court applied the Probation of Offenders Act and ordered that Four Star Pizza (Ireland) Limited pay €4,000 to Temple Street Children's Hospital in lieu of a conviction. The Office's prosecution costs were also recouped from the defendant.

Levet Limited T/A Fast Fit

This Office received a complaint in relation to the sending of unsolicited text messages by Levet Limited T/A Fast Fit. The Office had previously sent a formal warning to Levet Limited T/A Fast Fit in relation to its marketing operations.

In response to our investigations, Fast Fit admitted it did not have any evidence that it had obtained valid consent to send marketing text messages to the individual concerned. The Commissioner decided to prosecute Levet Limited T/A Fast Fit.

At the Dublin District Court on 22 April 2013, Levet Limited T/A Fast Fit pleaded guilty to one charge of sending an unsolicited marketing text message. The Court ordered the defendant to contribute €2,000 to the Jack and Jill Foundation and it applied the Probation of Offenders Act. The defendant agreed to pay the Office's prosecution costs.

Wexford Arts Centre

We received a complaint from an individual regarding an unsolicited marketing text message he received from Wexford Arts Centre. This message did not contain an opt-out mechanism for the recipient to opt out of the marketing database. In response to our investigation, Wexford Arts Centre informed us that, due to a combination of human error and technical difficulties, the marketing text message did not contain an opt-out. It told us that it had now removed the phone number from its database. On this basis, Wexford Arts Centre was issued with a formal warning with regard to its future marketing activities.

The same individual subsequently made a new complaint to this Office as he received yet another unsolicited marketing text message from Wexford Arts Centre despite being informed his number had been removed three months earlier. On this occasion, Wexford Arts Centre informed us that it had removed this individual's phone number but, due to human error, those changes had not saved correctly. The Commissioner decided to prosecute Wexford Arts Centre in relation to two offences:- failure to include an opt-out facility in a marketing text message (in respect of the first complaint) and sending an unsolicited marketing text message without consent (in respect of the second complaint).

At Wexford District Court on 22 July 2013, Wexford Arts Centre Limited entered a guilty plea in relation to both charges. The Court convicted Wexford Arts Centre Limited on one charge, it took the second charge into consideration and it imposed a fine of €500. The Court also ordered the defendant to pay €1,000 to this Office in respect of its prosecution costs.

Patrick Fox Hypnotherapy Limited

This Office received a complaint from an individual regarding an unsolicited marketing text message received from Patrick Fox Hypnotherapy Limited, a hypnotherapy clinic in Co. Meath. The marketing text message did not include an opt-out facility for the recipient to remove their number from the marketing database. The complainant informed us that she attended the clinic over three years previously and that she subsequently requested that her mobile number be deleted from its marketing contact list. We had previously sent a warning to Patrick Fox Hypnotherapy Ltd following a complaint from another individual. In that previous case, the complainant informed us that she received a marketing text message after placing an advertisement (unrelated to hypnotherapy services) containing her phone number in a local newspaper in the West of Ireland. That individual had no previous dealings with Patrick Fox Hypnotherapy Clinic.

In response to our investigation of the current complaint, Patrick Fox Hypnotherapy Clinic informed us that the text message in question was not intended as a marketing text message. However, it was clear to this Office that the message was marketing in nature as it offered discounts and promoted its range of treatments. The Commissioner decided to prosecute the case in light of the company's failure to heed the formal warning.

At Trim District Court on 26 September 2013, Patrick Fox Hypnotherapy Limited pleaded guilty in relation to the sending of an unsolicited marketing text message. The Court imposed a conviction and a fine of €1,000 on Patrick Fox Hypnotherapy Limited in relation to the sending of an unsolicited marketing text message without consent and it ordered the defendant to pay prosecution costs of €2,009.

Lex Software Limited T/A Legal and General Software

This Office received two complaints with regard to unsolicited marketing emails received from Lex Software Limited T/A Legal and General Software. One of the complainants had made a complaint to this Office about the same entity previously, having received unsolicited marketing emails from it in 2011. On that occasion Lex Software Limited T/A Legal and General Software was issued with a formal warning from us with regard to compliance in its future marketing activities.

In relation to the two current complaints, Lex Software Limited T/A Legal and General Software informed us that the complainants received unsolicited marketing emails due to human error. The Commissioner decided to prosecute the offences.

At Dublin District Court on 14 October 2013, a guilty plea was entered by the company on two charges – one for sending an unsolicited marketing email without consent and the second for failing to include in a marketing email a mechanism for opting out. The Court imposed a conviction in relation to both offences and it imposed fines of €200 on each offence. The defendant also covered this Office's prosecution costs.

Hanford Commercial Limited T/A The Maldron Hotel, Wexford

A complaint was received in this Office from an individual who informed us that he received an unsolicited marketing text message on his company mobile phone from Hanford Commercial Limited T/A The Maldron Hotel, Wexford. This occurred despite this Office being assured, on foot of a previous complaint from the same person three years previously, that the mobile phone number was removed from the company's database.

In response to our investigation, Hanford Commercial Limited T/A The Maldron Hotel, Wexford informed us that this error occurred due to a technical error whereby a manual block put on the complainant's number in 2010 did not carry through to a new account it had set up with its text service provider, Zamano. The Commissioner decided to prosecute Hanford Commercial Limited T/A The Maldron Hotel, Wexford for an offence under Regulation 13(4) of SI 336 of 2011.

On 14 October, 2013 at Dublin District Court, Hanford Commercial Limited T/A The Maldron Hotel, Wexford pleaded guilty to the sending of an unsolicited marketing text message to the complainant's company mobile phone. The Court convicted Hanford Commercial Limited T/A The Maldron Hotel, Wexford and it imposed a fine of €200. The prosecution costs were recovered by this Office from the defendant company.

Cherryhill Inns Limited T/A The Oliver Plunkett Bar, Cork

A complaint was received from an individual who received an unsolicited marketing email from Cherryhill Inns Limited T/A The Oliver Plunkett. The same individual had cause to complain to this Office regarding unsolicited marketing text messages she received from the same company over a year previously which she could not opt out of. In that previous instance, the company informed us that the complainant had signed up to receiving marketing messages and it produced a 'sign up' sheet which had her details entered on it. Having examined the sheet, the complainant informed us that she did not enter her details on it and that the handwriting on it was not hers. During that investigation the company agreed to remove the individual's contact details and it was issued with a formal warning by this Office with regard to compliance in its future marketing operations.

It was clear from the investigation of the current complaint from the same person that the company did not properly remove her contact details from its database. The Commissioner decided to prosecute the company. At Cork District Court on 22 October, 2013 Cherryhill Inns Limited T/A The Oliver Plunkett pleaded guilty to

three charges relating to the sending of an unsolicited marketing text message without consent, the sending of an unsolicited marketing email without consent and the sending of an unsolicited marketing text message without an opt out mechanism. The Court applied the Probation of Offenders Act conditional upon a charitable donation of €750 being made to the Cork Simon Community in respect of each of the three charges. Prosecution costs were recovered from the defendant.

Bord Gáis Éireann

We received a complaint from an individual regarding an unsolicited marketing email he received from Bord Gáis Éireann. This Office had previously issued Bord Gáis Éireann with a warning following the investigation of a complaint concerning unsolicited marketing phone calls made to an individual without his consent.

In response to our investigation, Bord Gáis Éireann informed us that, due to a manual error, an incorrect data file was used to send out the marketing email and, as a result, over nine hundred customers who had previously opted out of marketing communications were affected.

On 22 October 2013 at Cork District Court, Bord Gáis Éireann pleaded guilty to sending an unsolicited marketing email. The Court applied the Probation of Offenders Act conditional upon a charitable donation of €750 being made by the company to The Society of St. Vincent de Paul. Prosecution costs were recovered from the defendant.

Kearys of Cork

A complaint was received in the Office from an individual who received an unsolicited marketing text message from Kearys of Cork which did not include an opt-out option. The complainant said that he attended Kearys of Cork to have a car door fixed but he had not signed up to receive any promotional messages. This Office had previously warned Kearys of Cork with regard to its marketing operations following

the investigation of two complaints. In that warning we made it clear that we considered that the company had not obtained valid consent to send marketing communications to these individuals and we instructed it to perform a cleansing exercise on its marketing database to ensure that it was fully compliant with the marketing regulations.

In response to our current investigation, Kearys of Cork informed us that it was under the assumption that, since the complainant was an existing customer, that there was no issue in contacting him. It was apparent that the company had not taken appropriate remedial action following our previous warning with regard to obtaining valid marketing consents from customers and, accordingly, the Commissioner decided to prosecute the latest case.

On 22 October at Cork District Court, Kearys of Cork pleaded guilty to the sending of an unsolicited marketing text message. The Court applied the Probation of Offenders Act upon condition that the company make a charitable donation of €750 to the Cork Simon Community. Prosecution costs were recovered from the defendant.

TELECOMMUNICATIONS SECTOR

Eircom Ltd

We received complaints from two individuals who received unsolicited marketing phone calls from Eircom. The first complainant informed us that he had not been a customer of Eircom for many years and that he had opted out of marketing communications from the company. He made a complaint to Eircom directly and was informed that his details were removed from the telesales area and that it would not be contacting him again. Despite this assurance, Eircom phoned him for marketing purposes again, prompting him to complain to this Office. Of particular concern to us

was the fact that the complainant received a further marketing phone call from Eircom several weeks after the commencement of our investigation. In fact, during the course of our investigation, we had asked Eircom on three separate occasions prior to the making of the latest call to confirm that the complainant's number was removed from the marketing database.

Separately, a complaint was received from an individual who received a marketing phone call from an agent of Eircom on her landline number which was opted out of marketing on the NDD Opt-Out Register. On the same day, the agent called in person to her home as he was working as part of a "Feet on the Street" team. Eircom initially informed our investigation that it had no record of the call taking place. We subsequently traced the calling mobile phone number and we found that it was registered to the sales agent concerned.

In both cases, we were satisfied that Eircom did not have consent to make marketing phone calls to the individuals concerned and the Commissioner decided to prosecute Eircom for offences under Regulations 13(5)(a) and 13(5)(b) of SI 336 of 2011. Eircom pleaded guilty to two charges at Dublin District Court on 2 December, 2013. The Court imposed two convictions and it fined the company €1,500 on both charges. The company agreed to pay the prosecution costs incurred by this Office.

Meteor Mobile Communications Ltd (T/A Meteor)

This was the second successive year that Meteor was prosecuted by the Data Protection Commissioner for marketing offences. Having successfully prosecuted Meteor on 3 December, 2012 (see Case Study 12 in Annual Report 2012) a further offence was committed by Meteor on the following day by the sending of an unsolicited marketing text message to a customer whose mobile phone had been confirmed as having been opted out in November 2012. The individual also produced a copy of his original contract showing that he had opted out of receiving SMS marketing communications from Meteor.

The second case also involved a customer being sent unsolicited marketing text messages. In this case, the customer opted out of marketing in October 2012 and he received confirmation of his opt out from Meteor in November 2012. Despite that, he subsequently received three marketing text messages from Meteor. At the Dublin District Court on 2 December 2013, Meteor pleaded guilty to three charges of breaching Regulation 13(1) of SI 336 of 2011. The Court imposed three convictions and it fined the company €3,000 in respect of each of three charges. The company agreed to pay the prosecution costs incurred by this Office.

Telefónica Ireland Limited T/A O2

Two complaints were made to this Office in January 2013 from customers of O2 who received marketing text messages from O2 despite being opted out of marketing communications. During the course of our investigation of these complaints, O2 admitted that, due to an incorrect application of its consent for marketing rules, over 78,000 customers were sent marketing text messages in contravention of their marketing preferences.

In a separate complaint, an individual reported that he had received a marketing email in December 2012 from O2 to his email address which had been opted out of marketing communications from the company in April 2011. O2 informed our investigation that the agent who dealt with the opt-out request had processed the request on only one of two accounts held by the customer and that this led to him receiving a subsequent marketing email. At the Dublin District Court on 2 December, 2013 the company entered a guilty plea in respect of three charges for offences under Regulation 13(1) of SI 336 of 2011. In lieu of convictions, the Court ordered the defendant to make charitable donations of €2,000 to the Irish Wheelchair Association, €2,000 to the Children's Hospital, Crumlin and €2,000 to Pieta House. The company agreed to pay the prosecution costs incurred by this Office.

Vodafone

We received several complaints against Vodafone in 2012 and 2013. One customer reported to us in November 2012 that he had received a marketing phone call on his mobile phone despite it having been opted out of receiving marketing calls. The same customer had previously complained to us in February 2012 about receiving marketing calls from Vodafone and during the course of that investigation Vodafone confirmed to us in April 2012 that the customer's mobile number was now opted out. During the course of our investigation of this customer's current complaint, Vodafone admitted that its agent was negligent in applying the opt-out reference table when constructing a marketing campaign and this led to marketing calls being made to over 2,000 customers who had previously opted out of marketing.

A customer complained to us that he received marketing text messages even though his mobile phone was not opted-in to marketing. He explained that he was a Vodafone customer for landline and broadband services only and not for mobile phone services. He informed us that he had an issue with his landline on one occasion and he gave his mobile number to Vodafone in order to have an engineer contact him. Vodafone informed us that it had opted-in the mobile phone number to marketing. It confirmed that it opted the number out of marketing on 22 May, 2012. Despite this, the individual received a further marketing text message in June 2012. Vodafone explained that this occurred because the campaign team used an outdated table.

We received a complaint in October 2012 from a Vodafone customer who received marketing phone calls to his mobile phone during that month despite having received confirmation by email from Vodafone in September 2012 that his account had been unsubscribed from all marketing calls. During our investigation, Vodafone initially denied that the calls were made. We extended our investigation and we established from the service provider used by Vodafone that the calls were made as alleged by the complainant. Despite this, Vodafone continued to deny that any breach of the Regulations had occurred. Our investigation established that five offences had been committed in this case.

In May 2013, we received a complaint from an individual who continued to receive marketing phone calls to his mobile phone even though he had written confirmation

issued to him by Vodafone in September 2012 that his details were removed from its marketing database. After a four months delay, Vodafone informed our investigation that the letter issued in September 2012 confirming the opt-out preference was noted on the system by the agent who did not follow up on the opt-out action.

At the Dublin District Court on 2 December, 2013 Vodafone pleaded guilty to eleven charges – nine concerned breaches of Regulation 13(6) of SI 336 of 2011 in respect of unsolicited marketing phone calls to mobile phone and two concerned breaches of Regulation 13(1) in relation to unsolicited marketing text messages. The Court convicted Vodafone on seven charges and imposed fines of €3,000 on each charge. The Court applied the Probation of Offenders Act on four charges conditional on the defendant making donations of €3,000 to each of the following charities:- Irish Wheelchair Association, Laura Lynn Foundation, Children's Hospital Crumlin and Pieta House. The company agreed to pay the prosecution costs incurred by this Office.

Case Study 13: Access Request for CCTV footage

We received a complaint in February 2013 concerning the alleged failure of a data controller to supply a data subject, in response to an access request, a copy of their personal data and, in particular, the CCTV footage of an incident involving the data subject. The data subject provided the data controller with the specific date and time of the incident captured on the CCTV system.

A claims adjuster firm responded to the access request on behalf of the data controller stating that it was in possession of the CCTV footage but it was not in a position to release a copy of the footage as images of other customers were identifiable on it and to release same would contravene data protection rules.

We commenced our investigation in March 2013 by writing to the data controller. The claims adjuster subsequently replied to us and it stated that the supply of the CCTV footage could potentially prejudice any right of recovery or indemnity that it was due to receive. It also claimed that, as there were other members of the public in the CCTV footage, providing the footage to the data subject would breach the Data Protection Acts.

We responded to the claims adjuster and we informed it that it had not cited an exemption under the Data Protection Acts which it was seeking to rely on to withhold a copy of the CCTV footage. We also drew its attention to the judgment of the High Court in the case of Dublin Bus v The Data Protection Commissioner[10]. This case related to an access request for a copy of CCTV footage concerning a woman falling on a bus (Case Study 5 in Annual Report 2012 refers). The High Court ruled that "*the existence of proceedings between a data requester and the data controller does not preclude the data requester making an access request under the Act nor justifies the data controller in refusing the request."* We told the claims adjuster to re-consider its position on withholding the CCTV footage in light of that judgment.

On foot of our correspondence the claims adjuster sought photographic identification of the data subject in order to correctly identify him in the CCTV footage. On receipt

[10] [2012] IEHC 339

of photographic identification it released a series of photographic stills from the CCTV footage to the data subject's legal representatives. The data subject's solicitor wrote to our Office and informed us of their dissatisfaction that there was no audio recording supplied with the series of stills. We wrote to the claims adjuster about this matter and it informed us that there was no audio recorded on the data controller's CCTV system. We advised the data subject's solicitor that we were satisfied that the obligations of a data controller were met in this case by providing a reasonable series of stills of images from the CCTV footage showing the requester's image only.

The following outlines this Office's position with regard to access to CCTV footage made under a Section 4 access request:

1.Any person whose image is recorded on a CCTV system has a right to seek and be supplied with a copy of their own personal data from the footage.

2.When making an access request for CCTV footage, the requester should provide the data controller with a reasonable indication of the timeframe of the recording being sought - i.e. they should provide details of the approximate time and the specific date(s) on which their image was recorded. For example, it would not suffice for a requester to make a very general request saying that they want a copy of all CCTV footage held on them. Instead, it is necessary to specify that they are seeking a copy of all CCTV footage in relation to them which was recorded on a specific date between certain hours at a named location. Obviously, if the recording no longer exists on the date on which the data controller receives the access request, it will not be possible to get access to a copy. Requesters should be aware that CCTV footage is usually deleted within one month of being recorded.

3.For the data controller's part, the obligation in responding to the access request is to provide a copy of the requester's personal information. This normally involves providing a copy of the footage in video format. In circumstances where the footage is technically incapable of being copied to another device, or where the supply of a copy in video format is impracticable, it is acceptable to provide stills as an alternative. Where stills are supplied, it would be necessary to supply a still for every second of

the recording in which the requester's image appears in order to comply with the obligation to supply a copy of all personal data held.

4.Where images of parties other than the requesting data subject appear on the CCTV footage, the onus lies on the data controller to pixilate or otherwise redact or darken out the images of those other parties before supplying a copy of the footage or stills from the footage to the requester. Alternatively, the data controller may seek the consent of those other parties whose images appear in the footage to release an unedited copy containing their images to the requester.

5.Where a data controller chooses to use technology to process personal data, such as a CCTV system to capture and record images of living individuals, they are obliged to shoulder the data protection obligations which the law places on them for such data processing. In the matter of access requests for CCTV footage, data controllers are obliged to comply fully with such requests. Claims by a data controller that they are unable to produce copies of footage or that stills cannot be produced from the footage are unacceptable excuses in the context of dealing with an access request. In short, where a data controller uses a CCTV system to process personal data, its takes on and is obliged to comply with all associated data protection obligations.

Case Study 14: Data Security Breach at Loyaltybuild Ltd.

Breach Notification

On the 1st November, 2013, the Office received a data security breach notification from Loyaltybuild Ltd. in accordance with our Personal Data Security Breach Code of Practice. The notification informed this Office that encrypted credit card data had been compromised through an attack on its website.

Loyaltybuild Ltd is a company (data processor) who provides a service facilitating hotel getaway breaks that are offered as part of loyalty schemes run by its clients (data controllers).

The Office also received breach notifications from two data controllers in relation to the same matter.

On the 11th November 2013, Loyaltybuild Ltd updated their notification to inform the Office that credit card details (full card number, expiry date, card holder name and CVV code), in unencrypted format, and also contact details for customers who had made bookings through the Loyaltybuild website, had also been compromised. Data controllers across Europe were affected by the breach. Data was compromised to varying degrees, in some cases it included unencrypted credit card data, while in other cases it was confined to customer contact details.

For completeness of reporting on the investigation, this case study spans 2013 and the early months of 2014.

Actions taken by the Office - Inspection 12th November 2013, Enforcement Notice 13th November 2013, information campaign to affected individuals

An Inspection Team from the Office carried out a site visit of Loyaltybuild Ltd on the 12th November 2013. The Inspection team found serious issues regarding the security of data on Loyaltybuild's systems and a lack of procedures to ensure that the data was protected and managed properly. Loyaltybuild advised that it had been inadvertently recording full credit card details in unencrypted format and that it was not a part of their recorded process.

On foot of the report of the Inspection Team, the Commissioner issued an Enforcement Notice against Loyaltybuild Ltd on the 13th November, 2013. The Enforcement Notice was part of a package of immediate actions undertaken by the Office to limit the affects of the data security breach.

The actions required by the Enforcement Notice were as follows:

- Loyaltybuild was required to notify all its clients about the security breach and advise them to notify affected individuals.
- Loyaltybuild was required to delete all personal data held for the purpose of providing services to its clients.
- Loyaltybuild was required to achieve PCI-DSS compliance[11] in respect of its processing of payment card data, verified by an independent third party.
- Loyaltybuild was to implement a series of changes to its procedures to bring them in line with industry best practices.
- Loyaltybuild was not allowed process personal data until it had satisfied this Office that these requirements were being met.

The Office also liaised with a number of banks and the Irish Payment Services Organisation (IPSO) to determine the potential implications for affected individuals. Based on this information, we issued advice to individuals, both through the Office website and media interaction, to monitor their bank accounts and to ensure that they could identify all payments being processed against their debit / credit card and notify their card company of any unusual activity. Affected individuals were also warned to be wary of any unsolicited communication they received.

Loyaltybuild Ltd's remedial actions in relation to procedures and policies

Loyaltybuild Ltd. has been in regular contact with the Office advising of its progress on the matters set out in the Enforcement Notice and has cooperated fully with the Office's investigation.

In accordance with the requirement in the Enforcement Notice, Loyaltybuild Ltd employed a company to carry out its PCI Certification. On receipt of the Report of

[11] Payment Card Industry Data Security Standard

Compliance, this Office employed a further company to carry out a peer review of the report.

A further requirement was put in place that Loyaltybuild Ltd. engage a third party auditor to scrutinise its procedures and policies (choice of company to be subject to final approval by this Office). The Office consulted with that company to satisfy ourselves of their competence in respect of carrying out a system-wide audit and subsequently approved their use.

The requirements of the system-wide audit were set out by the Office and we met with the company to discuss the implementation of this audit. The audit will continue over a number of months in 2014. The company will provide us with regular updates.

A particular issue addressed by the Office was the handling of credit card payments. Our Inspection Team advised Loyaltybuild Ltd to consider alternative processes to retaining credit card details on their systems. Loyaltybuild Ltd. no longer stores credit card details. This process was verified by our Inspection Team. Instead of processing the credit card payments themselves, Loyaltybuild Ltd. will now pass the customer on to a third party processor's website, which specialises in credit card payments.

A further visit by an inspection team to Loyaltybuild Ltd. in late January 2014 verified that the terms of the Enforcement Notice had been met, and the Commissioner lifted the Enforcement Notice to allow Loyaltybuild Ltd. to recommence processing personal data.

Data Controllers

The Investigation of the breach necessarily involved an assessment of any data protection issues in the relationship between the various data controllers with whom Loyaltybuild Ltd had contracts as a data processor.

Loyaltybuild had contracts with data controllers across Europe. This Office can only interact with data controllers based in this jurisdiction. However, we notified relevant Data Protection Authorities (DPAs) so that they could contact data controllers in their jurisdiction. Relevant DPAs were provided with regular updates on our investigation.

We found it necessary to focus on the contracts in place between the various data controllers based in this jurisdiction and Loyaltybuild Ltd.

The biggest issue we found among the data controllers we examined was a lack of understanding of their status as data controller, in relation to their customers who booked hotel breaks through the Loyaltybuild website. All the data controllers we spoke with initially believed that Loyaltybuild was the data controller. This Office explained to them their responsibilities as a data controller and that Loyaltybuild was a data processor in respect of the loyalty breaks offered by the companies. We explained that when the customer (data subject) booked a hotel break, they did so as a customer of the data controller and that Loyaltybuild was only a processor.

We looked at the contracts in place between the data controllers and Loyaltybuild under a number of headings;

- Did the contract specify ownership of data
- Did the contract specify a retention period
- Did the contract require compliance with DP legislation
- Did the contract specify appropriate security requirements
- Did the contract require confidentiality of data
- Did the contract restrict further processing
- Did the contract specify actions to be carried out on receipt of a Subject Access Request
- Did the contract specify the deletion of data
- Did the contract specify actions on termination of contract
- Did the contract allow for the right to audit the data processor

We found that in all cases there were issues with one or more of the above. We found that no Data Controller had set a Retention Policy, setting out the timeframe for holding data in respect of its customers.

ODPC also requested details on what "due diligence" had been carried out prior to awarding the contract. Again this Office identified issues with some data controllers who failed to carry out proper due diligence.

Along with the Enforcement Notice issued to Loyaltybuild, the Commissioner also issued Enforcement Notices to two Data Controllers on the 13th November 2013. These Enforcement Notices required affected individuals to be notified, detailing the nature of the data and the steps to be taken to secure their personal and financial data. They were also required to ensure that any data processor acting on their behalf that carries out financial transactions involving customers is PCI compliant as required.

Main Findings of Loyaltybuild Ltd Investigation:

- Loyaltybuild Ltd. failed to implement adequate security measures to protect the data it held on its systems
- Loyaltybuild Ltd. failed to implement proper procedures to manage the data it processed.
- Data Controllers were unaware of their role in the control of the data held on Loyaltybuild Ltd.'s systems.
- No Data Controller had set a Retention Policy, setting out the timeframe for holding data in respect of its customers.

Case Study 15: Client list taken by ex-employee to new employer

In January, 2013 we received a complaint from an individual in relation to receipt of unsolicited correspondence to her home address, from a company with whom she had no business relationship. The correspondence referred to the individual's existing pension plan with another company and offered a review of the individual's existing assets or advice concerning her future provision. The letter also indicated the sender's intention to phone the recipient to discuss the matter further. The individual stated that she was annoyed and aggrieved that her personal and financial details were now in the hands of a company of which she had no knowledge.

The individual contacted the company with which she had set up her pension plan and they confirmed to her that the person who had sent her the unsolicited letter had left their employment in December 2011.

Section 2 of the Data Protection Acts, 1988 and 2003 (the Acts), provides that personal data shall be fairly obtained and processed and shall not be further processed without the prior consent of the individual concerned. We asked the new employer to confirm whether the employee had brought in data relating to clients that he obtained from his time working in his previous employment. We also asked the new employer to confirm what consent, in line with the Data Protection Acts, it had to process such data.

Our letter also informed the new employer that it should be aware that contacting an individual by phone, for the purposes of electronic direct marketing, without first receiving their consent, is an offence under Statutory Instrument No 336 of 2011.

The new employer confirmed that, having conducted its own internal investigation into the matter, that approximately fifty former contacts of the employee were written to. It stated that no follow up phone calls were made. The new employer confirmed that any such data that the employee possessed had been destroyed and that no further attempts would be made to contact those individuals.

The complaint was resolved on an amicable basis when the company provided this Office with a letter of apology dated 28 January, 2013 to forward, on its behalf, to the individual concerned.

However, in early April, 2013 this Office received a data security breach notification from the former employer informing us that another of their clients had informed them that she had received a letter from one of its former employees soliciting business. The nature of the letter, although addressed to a different client, was similar to the incident previously investigated by this Office in January 2013. The letter was dated 15 January, 2013 thus predating the confirmation of 28 January, from the new employer, that the client data had been destroyed.

Our investigations of such instances are twofold. We contact the company responsible for sending the unsolicited correspondence and we also deal with the company responsible for the data, to determine whether the security procedures it has in place to protect against the unauthorised access and disclosure of personal data are sufficient.

In this instance we requested the former employer to inform us of the policies it had in place regarding the security of client information in circumstances where an employee is moving to a new employment. We also requested to be provided with a copy of the data protection element of the contract of employment.

When providing this Office with a copy of the Confidentiality and Solicitation agreement signed by the former employee, the former employer also provided us with a copy of another letter sent to one of their clients by the former employee. The letter was dated 15 April, 2013 and was similar in nature to the letters sent to individuals in January 2013. However, on this occasion, the unsolicited correspondence made no reference to contacting the individual by telephone.

This information contradicted the confirmation we had received from the new employer in January 2013 that all data relating to the employee's previous employment had been destroyed. On becoming aware of this development, this Office had no option but to have two of our Authorised Officers carry out a site inspection, as

provided under Section 24 of the Acts, at the premises of the company. To assist with the site inspection, we requested the former employer to provide us with a copy of the client list of the former employee.

The purpose of the site visit by the Authorised Officers was twofold. Firstly to ascertain how it happened that a letter dated 15 April, 2013 issued to a client of the former employer, despite assurance from the new employer, in a letter dated 28 January, 2013 that all client data from their employee's previous employment had been destroyed. Secondly to carry out a search of the company's systems to satisfy ourselves that there was no further data in the company's possession relating to the clients of the previous employer. Using the data provided by the original employer, the Inspection Team carried out a search on the computer systems for individuals' names and addresses. The Inspection Team was satisfied that no further customer data remained.

We informed the new employer, on the morning of the site inspection, of our intention to visit his place of business that afternoon. We had not informed the new employer, prior to the site visit, of our knowledge of the letter dated 15 April, 2013. The new employer cooperated with the inspection.

Our investigation of the matter concluded on the basis of our receipt of written confirmation in May 2013 from the Managing Director of the new employer, stating that he fully accepted that breaches had occurred and outlining the actions his company was taking to prevent a recurrence. The Managing Director also confirmed that he personally oversaw the destruction of the data held by the employee.

This Office has noticed a significant increase in the number of data security breach notifications we are receiving in relation to this type of matter. We may first become aware of the matter via the receipt of a complaint from an individual relating to their receipt of unsolicited communications or from our receipt of a data security breach notification from the data controller. While there are obvious business related implications to such incidents, the focus of this Office's investigation concerns the basic principles of data protection relating to security, fair obtaining and processing of personal data.

Case Study 16: Loss of photocopies of passports

In November 2013, a voluntary organisation that is involved with young people notified us of a data security breach relating to the loss by one of its local groups of photocopies of passports. The organisation informed us that one of its local groups had reported that a file containing photocopies of individual passports for 44 young people and leaders, and 38 Parental Consent forms, was lost or mislaid on the return journey from a trip abroad the previous August. We were informed that the Volunteer in charge only became aware of the loss of the documentation in November.

The three pronged approach from this Office when dealing with personal data security breaches is that we expect that the Data Controller,
1. Informs the affected individuals (including what information was disclosed)
2. Secures the data in question and,
3. Informs this Office of steps taken to reduce the risk of a similar incident reoccurring.

As the whereabouts of the documentation was unknown this prevented the data controller from securing the data.

The organisation confirmed that it was arranging immediately to contact the parents to advise them of the loss. As per the provision of the Code of Practice, this allows the individuals to consider the consequences for each of them individually and to take appropriate measures.

This Office queried the reason why the organisation considered it necessary to hold photocopies of the passports. We informed the organisation that we did not consider the photocopying of the passports to be best practice. The organisation confirmed that it too was questioning why passports were being photocopied and was investigating the extent of this practice within the organisation. It put forward the suggestion that perhaps the purpose of photocopying the passports was done as a precaution in case the original passports were lost while abroad. We also informed the organisation that,

even if it was in a position to provide a legitimate basis for the photocopying of the passports, the documents should have been destroyed once the trip abroad was over. This procedure would have alerted the Volunteer sooner to the loss of the documents.

The Personal Data Security Breach Code of Practice also provides that, in appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects. In this regard, this Office, for the benefit of our own understanding of the matter, contacted the Passport Office, Department of Foreign Affairs. The purpose of our communication with the Passport Office was to seek advice on the potential implications of the loss of a photocopy of a passport and whether this was an issue that should be reported to the Passport Office.

The Passport Office advised that there was a possibility that a photocopy of passport details, if it fell into the wrong hands, could be used to create a duplicate as a fraudulent document. The Passport Office advised that the affected passports could be put on the Department of Foreign Affairs "check list". This Office understands that this involves the placing of a computer block that means when an individual reapplies for a passport, a double check is carried out on the application.

Our investigation of the data security breach concluded on receipt of confirmation from the organisation that it had written to all the parents advising them of what had been lost. The organisation also informed us that a parents meeting had been held. The organisation also confirmed that it had taken advice from the Department of Foreign Affairs and was preparing guidelines for its groups on the issue of the handling of passports.

This case demonstrates the basic principles of data protection in relation to data security and the requirements under the Data Protection Acts 1988 & 2003 (the Acts), for a data controller to have a clear purpose in relation to the obtaining and retention of personal data. In this instance it was not clear why the local group had photocopied the passports. The Acts provide that the data should be obtained only for one or more specified, explicit and legitimate purposes. The Acts also provide that the data shall not be kept for longer than is necessary for the purpose for which it was initially

obtained.

Case Study 17: Medical files sent to incorrect email address

The Office received a data security breach notification from a G.P. which reported that an email containing a patient file had been sent to an incorrect recipient. This was the result of a typographical error when entering the email address. The patient file was exported from the software system used by the G.P and attached to the email. The data controller became aware of the matter when the intended recipient contacted the data controller advising that they had not received the email.

The data controller advised our Office that they had notified the affected individual of the matter.

As part of our investigation into the matter, we contacted the software supplier to determine how easy it would be for a third party to access a patient file exported from their system. The software company stated that only an individual with a registered copy of their software could open or access the patient file. The file would have to be imported into the software system to be read. Our Office asked whether there was any other software that could be used to open the file. We were advised that the file could not be opened in a legible format outside of their own software.

The data controller also advised our Office that, as a means of preventing the repeat of such an incident, it proposed that, where it was sending a patient file to another G.P., that the receiving G.P. must first send it an email requesting the patient file. The data controller can then reply directly to the email, ensuring the correct address is used.

The data controller also sought our advice on raising this issue in a public forum as a means of raising awareness of the dangers. We responded by stating we had no objections to such a course of action, provided that no personal data was disclosed. As our Office was advised by the software company that the email could not be accessed by the recipient, we recorded the matter as a non-breach.

This issue highlights the necessity for sending sensitive data, such as medical data, via a secure means. It shows how easy it is for emails to be issued to an incorrect recipient and without some means of securing the data contained within the email, could be disclosed to an unauthorised party.

Case Study 18: Computer affected by Ransomware

Our Office received a notification from a Medical Practitioner that their computer system had been compromised by Ransomware.

Ransomware is a malicious file which is designed to extort money from a user by disabling their computer or encrypting files stored on the computer. The user is then informed that they must pay to have the files restored. There is a risk that after paying the "ransom", the user will not regain control of their system.

The data controller notified the Office that they were unable to access their computer system, due to the Ransomware that had been installed on their systems. This meant that they were unable to access their patient files. They also advised the Office that they had received a demand for €5,000 in return for the re-instatement of the data. The data controller stated that they had informed An Garda Síochána and had not paid the ransom.

The data controller, on discovering the issue, alerted their IT service provider. After an initial investigation, a third party IT service provider was also employed to help recover the data. During this process, the data controller discovered that backup data for the previous five months had also been compromised. The data controller had therefore lost all patient data obtained in the previous five months.

Our Office contacted the data controller and asked that we speak directly to the IT service provider to determine how the backup tapes going back over a period of five months had been compromised. The IT service provider informed us that there were two separate backup facilities in place. Firstly, there was an on-site hard drive device that was written to each night. Secondly, there was a system of backup tapes in place, which were then stored off-site.

The on-site hard drive had been affected by the Ransomware software. However, it was discovered that the backup media tape system had not actually been recording, but there were no alerts issued by the backup software to identify an issue.

We sought assurance from the IT service provider that the data had not been exported by the Ransomware. The IT service provider stated it had found no evidence to suggest that the data had been taken from the data controller.

It was noted that the data controller had a basic firewall in place and an up-to-date anti virus system. The data controller had also set aside a budget for an upgrade to their computer systems to take place later in the year.

The data controller informed this Office that it was preparing to notify all its patients. We recommended that the notification be directed to those individuals for whom records had been compromised. Any patients who had not attended the practice since the last viable backup tape was created were not affected by the security breach as their records were not compromised.

It was clear that the data controller had installed systems to protect the data under its control and was planning on upgrading the systems. However, it is imperative that, when systems are implemented, they are checked on a regular basis to ensure they are operating correctly.

Case Study 19: Customer had on-line access to third party telephone bill details.

The Office received a breach notification from a telecommunications provider notifying us of a personal data security breach under the provisions of Commission Regulation (EU) No 611/2013 of 2013.

This Regulation imposes a legal obligation on providers of publicly available electronic communications networks or services to notify this Office of a personal data security breach, no later than 24 hours after the detection of the breach, where feasible.

The Service Provider informed us that one of its customers, who was a member of an organisation, while reviewing his telephone bill via the Provider's on-line facility, noticed that he had access to the details of bills of over 400 other members of the same organisation. On becoming aware of the incident, the Service Provider quickly removed a shared billing code that linked a limited number of accounts related to members of the organisation on the Service Provider's billing system.

The Service Provider informed us that it was able to confirm from the customer's log-in details that he had access only to customers' name, surname, mobile number and six months call records. We were informed that the customer did not have access to the individuals' financial details or address details.

The root cause of the incident was identified as being a customer service agent applying a shared billing code via the administration systems. We were informed that the agent incorrectly set up the shared billing code resulting in the accounts being linked in error and making the individual who accessed the data the master account holder.

The Service Provider confirmed that it was informing all individuals affected by the incident. The Service Provider also informed the individuals that the matter had been rectified and had ensured that a similar incident would not occur again.

This case demonstrates how the speed at which a breach is identified and dealt with may assist in minimising the overall security risk of the breach. Informing the affected individuals of the matter permits them to consider the consequences for each of them individually and to take appropriate measures as they see fit. The reporting of the matter to us by Data Controllers as speedily as possible, as per the above legislation, also assists in our role of trying to improve compliance with Data Protection legislation.

Appendices

Appendix I – Presentations

Appendix 2 – Registration Statistics

Appendix 3 – Account of Income and Expenditure

Appendix 4 – Energy Report

Appendix 1- Presentations and talks

During 2013 the Commissioner and staff of the Office gave presentations to the following organisations:

Educational

Association of Secondary Teachers in Ireland
Irish Second-Level Students Union
Rathdown School
University College Dublin
Admissions Officers Association
Dublin Institute of Technology – third level disability officers
Mullingar Community College
Carlow IT

Commercial

American Chamber of Commerce Ireland
Digital Repository of Ireland
Security Institute of Ireland
South-East Regional Authority

Voluntary

Children's Rights Alliance
Council of Irish Adoption Agencies

Health Sector

Royal College of Physicians of Ireland
Irish Pharmaceutical Healthcare Association
National Nursing Home Development & operation conference
Nursing Homes Ireland
Royal Academy of Medicine in Ireland
TCD Health Informatics Course
RCSI-Clinical Research Nurse Programme

International

Academy of European Law
American Bar Association x2
Centre for Information Policy leadership x2
Conference of Data Protection Commissioners
Dublin Web Summit
European Archives Group
European Privacy Association

European Public Administration Network
Federation of European Academies of Medicine
India Centre for Internet Society
International Association for Media and Communications
International Association of Privacy Professionals x3
Macedonian DPA
Privacy Law and Business
TAIEX Macedonia x 2
TAIEX Croatia
TAIEX Workshop on Civil & Criminal Liability for violating the right to personal data protection, Macedonia
Norwegian Consumer Ombudsman's Office

Legal

Bar Council of Ireland
CPD Board Ltd x2
Law Society
Legal-Island
Matheson Solicitors
TechLaw
The Law Society of Ireland

Mixed Seminars

Cyber &Data Security Conference
Family On-Line Safety Institute
Information Security World Conference
Irish Association of Social Workers
Irish Computer Society
Irish Penal Reform Trust
North Dublin Chamber of Commerce
PDP Practical Compliance Conference
Secure Computing Forum
Institute of International and European Affairs
DJER - Taking Care of Business Seminar

Government/Agency

Department of Environment
Fine Gael Parliamentary party
Institute of Public Administration x2
Office of Comptroller and Auditor General
Galway Citizens' Information
PIBA
POBAL
Oireachtas Committee on Health and Children

Appendix 2 – Registrations 2013

The total number of register entries in 2013 was 5,778. This figure can be broken down into the following categories:

(a) Financial and Credit Institutions
614

(b) Insurance Organisations
354

(c) Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts.
95

(d) Telecommunications / Internet Providers
46

(e) Health Sector
1914

(f) Pharmacists
1091

(g) Miscellaneous
512

(h) Data Processors
1152

Total number of registration entries

2011	**2012**	**2013**
4940	**5338**	**5778**

In 2013 the number of organisations registered increased by 440 approximately 8%. This increase arose due to a targeted awareness campaign on the Health Sector and also pursuit of the cases which had gone off the Public Register during 2013.

Appendix 3 - Abstract* of Receipts and Payments in the year ended 31 December 2013

Account of Receipts and Payments in the year ended 31 December 2013

Receipts	**2013** **€**	**2012** **€**
Moneys provided by the Oireachtas	1,960,999	1,552,468
Fees	660,290	615,023
Other Receipts	nil	1,915
	2,621,289	**2,169,406**
Payments		
Staff Costs	1,620,359	1,265,509
Establishment Costs	131,631	68,232
Legal and Professional Fees	179,050	206,633
Audit Fees	_____	3,600
Miscellaneous Expenses	29,959	8,494
	1,960,999	1,552,468
Payment of receipts for the year to the Vote for the Office of the Minister for Justice and Equality	638,829	604,645
Receipts payable to the Vote for the Office of the Minister for Justice and Equality at year end	21,461	12,293
	2,621,289	**2,169,406**

*The figures for 2013 outlined above are still subject to audit by the Comptroller and Auditor General. The final audited accounts will be presented to the Minister for Justice & Equality for presentation to the Oireachtas

Appendix 4 - Energy Report

Overview

The Data Protection Commissioner's Office is part of a building which was built in 2006. We occupy the first floor of the building with a floor area of 13.38 square metres. Currently, 31 members of staff are accommodated in this area.

In 2013, the sources of the main usage of energy in the Office were gas and electricity for heating, lighting and other uses.

In 2013 the Energy rating for the building was C1.

Actions Undertaken

During 2013 the Office appointed an Energy Officer who received the necessary training from Sustainable Energy Authority of Ireland (SEAI). We have participated in the new SEAI on-line system 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 2013:

Usage	111,719kwh
Non Electrical	62,919kwh
Electrical	48,800kwh

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

During 2013, additional staff were assigned to the Office. The consequent redesign of the Office into a largely open plan area has resulted in a need for additional heating. We have begun the process of introducing an extension to our existing permanent gas heating system, to obviate the need to use portable heaters. Light bulbs are replaced with energy-saving bulbs when replacements are required. We will continue to explore further ways of reducing energy usage.