An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Twenty-Third Annual Report of the Data Protection Commissioner 2011

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

PRN. A12/0071

List of tables and figures

Part 1

Foreword

Since its establishment in 1988, our Office, under successive Commissioners, has tried to use the resources allocated to it to best achieve the duties assigned to it by law. These resources have always been modest – amounting at present to a budget of only €1.5M and a staff of 22. We have sustained significant cut-backs in our budget in recent years. We have done our best to prioritise our resources to those activities likely to lead to the greatest return in terms of improved protection of data protection rights. For so long as our responsibilities were largely confined to protecting the rights of Irish residents, operating with limited resources was difficult but tolerable.

The scope of our responsibilities has changed significantly in the past 3 to 5 years. This arises in particular from the success of the Industrial Development Authority in attracting to Ireland companies conducting significant processing of personal data. We have worked with these companies to help them understand their obligations under EU data protection law towards all EU users of their services.

The legislative proposals presented by the European Commission[1] in January of this year, if passed into law, will involve increased responsibilities for our Office under the so-called "one-stop-shop" arrangement for multinational companies providing services to EU users from an Irish base. While the exact division of labour between data protection authorities has yet to be finalised, it clearly will involve a greater degree of responsibility for our Office in relation to multinational companies which choose Ireland as an EU base. Failure to adequately discharge this responsibility will carry significant reputational risks for the country.

The implications of our increased European responsibilities were brought home to us forcefully in relation to our audit of the activities of Facebook-Ireland. Facebook-Ireland had unambiguously placed itself under our Office's jurisdiction through changes in its contractual arrangements with its EU users and the establishment of clear responsibility for the processing of their data. We therefore included them in

[1] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

our programme of audits for 2011. This was the most complex audit ever undertaken by our Office, involving about a quarter of our staff resources for 3 months and external technical assistance from University College Dublin (UCD). It would have been impossible without the enthusiasm and dedication of the audit team, led by Deputy Commissioner Gary Davis and the expertise of Dave O'Reilly of UCD.

We clearly cannot maintain a similar level of commitment in relation to other multinational companies without additional resources. I am confident that this message is understood by the Government and would hope to be allocated additional resources in the course of this year.

I thank the staff of the Office for their work during the year and for maintaining their positive commitment to serving the needs of our many customers despite the pressures they have been under.

Billy Hawkes
Data Protection Commissioner
Portarlington, April 2012

Introduction

As outlined in my foreword the data protection landscape is changing. We are now seeing a definite shift in the nature and type of complaints received by the Office from the traditional complaint related to inappropriate or unfair use of personal data to a clearer technology focus with individuals concerned about the security of their personal data and the uses made of that data by software and technology applications. Last year for the first time the number of data breach notifications outstripped the number of complaints opened for investigation (by six). The need to deal with the reality of the potential impact on individual privacy and data protection rights which can be caused by poorly thought out technology is in many respects the back-drop to the European Commission's proposals for a new uniform Data Protection Regulation that will apply across all EU Member States. In this respect the current allocation of resources in my Office is as outlined below. I expect in the coming years to see significant re-alignment of where those resources need to be deployed to best effect.

Allocation of Resources

Note: Staff costs = 85% of Budget

Investigations & Enforcement[2]	35%
Guidance & Education[3]	25%
Audits/Inspections	15%
Notifications[4]	10%
EU/International Cooperation	10%
Administration[5]	5%

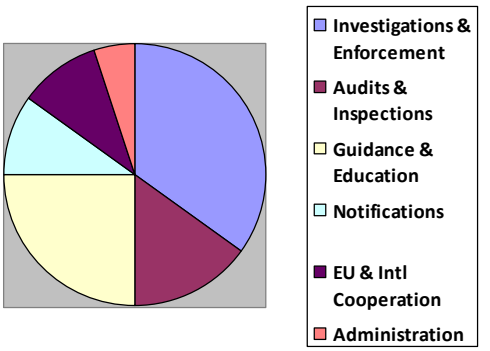
[2] Includes investigating complaints and data breaches; issuance of Enforcement Notices; prosecuting offences under the Data Protection Acts and the Electronic Privacy Regulations

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

[4] 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

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

Figure 1 Allocation of Resources (approximate)



Customer Service

This year, once again, my 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 from members of the public on a very broad range of issues, from access rights to registration obligations. Emails were the next most common source of queries with a smaller number of queries received by post. In addition, we held some 244 meetings with external organisations and attended some 33 EU and international meetings which this Office is statutorily obligated to attend in many instances.

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 point of information which we review and update regularly to make sure that relevant data protection developments are highlighted to visitors to it.

In the last 12 months, we have given 53 presentations to various organisations, details of which are available in Appendix 1– Presentations & Talks.

We continue to place great value on our interaction with the media as this provides a valuable platform for raising awareness among the public of data protection issues.

Last year my Office dealt with some 400 queries from the media. This in part reflects the extraordinary media attention around the world on our investigation and subsequent audit of Facebook but domestically the media interest in data protection matters has also significantly increased.

Irish Language Scheme

Our most recent Irish Language Scheme under the Official Languages Act 2003 was put into effect in 2010 and will be in effect until 2013. We continue to maintain our commitment to provide an effective service 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 & Equality - payroll, general payments, HR, and IT (Citrix) - which are subject to that Department's procedures. The Office is also subject to the Department's internal audit system. In so far as matters under its control are concerned, the Office is in full compliance with the requirements of the Code.

Complaints and Investigations

During 2011 my Office opened 1,161 complaints for investigation (183 complaints related to a co-ordinated action against one data controller with regard to access rights). This was a record high number of complaints and it compares with 783 complaints in 2010. As referenced in our recent reports we actually receive a multiple of the number of complaints which are actually opened for formal investigation. Often it is possible to conclude such complaints informally or they do not meet the criteria on which an investigation can be grounded.

The number of complaints under the Privacy in Electronic Communications Regulations (S.I. 535 of 2003 (as amended) and S.I. 336 of 2011) was in line with the

trend of recent years. In 2011 we opened a total of 253 complaints in this category relating to unsolicited direct marketing text messages, phone calls, fax messages and emails. This compares with 231 such complaints in 2010 and 262 in 2009. As I indicated in 2010, a trend has emerged in the past few years with regard to the use of unsolicited text messages as a form of marketing by businesses across almost every sector of the economy. A large portion of the 253 complaints received in 2011 with regard to unsolicited electronic communications related to marketing text messages sent by businesses large and small in Ireland. Complaints about unsolicited email marketing messages sent by Irish businesses are also on the increase. During the course of our investigations of these complaints we invariably find that the offending businesses concerned are unaware of the law which applies to such communications with regard to subscriber consent and the requirement to provide an opt-out mechanism in each marketing message. As in the past, I will use my prosecution powers against entities who persist in infringing the law and I have included case studies on all prosecutions brought in 2011. In total there were 54 prosecutions initiated against 6 entities.

As in previous years, the vast majority of complaints concluded in 2011 were resolved amicably without the need for a formal decision under Section 10 of the Acts or prosecution under the *e*Privacy Regulations where relevant[6]. In 2011 I made a total of 17 formal decisions on whether there had been a contravention of the Data Protection Acts. 13 of these fully upheld the complainant's assertion that there had been a breach, 1 partially upheld the assertion and 3 rejected the assertion. 1080 investigations of complaints were concluded in 2011 (Figure 2).

Table 1 shows the breakdown of complaints by data protection issue. Excluding the 253 complaints (approx 22%) concerning breaches of the *e*Privacy Regulations, the remainder (approx 78%) relate to breaches of the Data Protection Acts, 1988 & 2003. Complaints concerning access rights accounted for approximately 48% of the overall total. A total of 562 complaints (including the 183 single data controller complaints referred to above) about access rights were opened in 2011, compared with 259 in

[6] Breaches of the Regulations are, for the most part, criminal offences which can be prosecuted through the Courts, leading to fines. Breaches of most of the provisions of the Acts are not offences. The law does not provide for the direct imposition of financial penalties by the Office

2009, 312 in 2008 and 187 in 2007. This upward trend reflects a growing level of public awareness of the right of access to personal data. Table 2 gives details of the number of complaints received on an annual basis since 2002.

Table 1 Breakdown of complaints opened

2011 - Breakdown of complaints opened by data protection issue

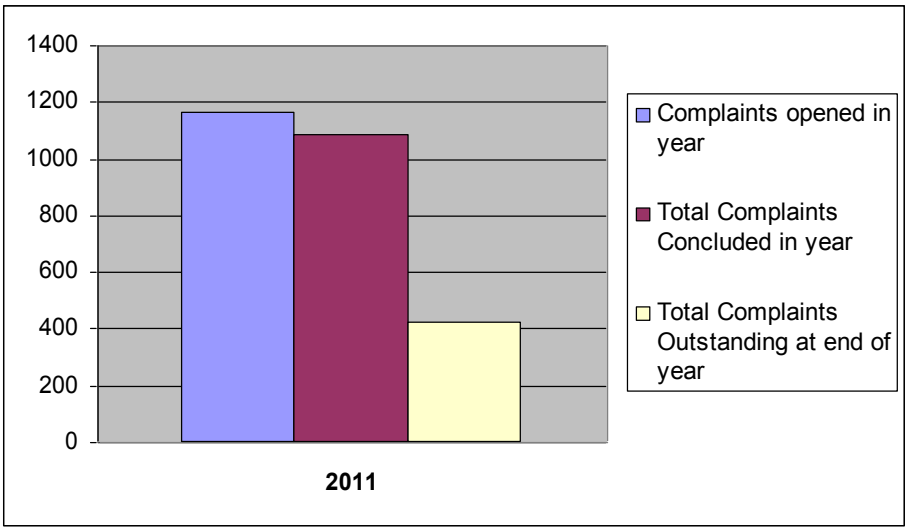
	2011 Percentages	Totals
Access Rights	48%	562
Electronic Direct Marketing	22%	253
Disclosure	10%	118
Unfair Processing of Data	6%	62
Unfair Obtaining of Data	4%	42
Use of CCTV Footage	3%	37
Failure to secure data	2%	25
Accuracy	1%	14
Excessive Data Requested	1%	14
Unfair Retention of Data	1%	12
Postal Direct Marketing	1%	11
Other	1%	11
TOTAL	**100%**	**1161**

Table 2 Complaints opened for investigation since 2002

Complaints opened for investigation since 2002

Year	Complaints Opened
2002	189
2003	258
2004	385
2005	300
2006	658
2007	1037
2008	1031
2009	914
2010	783
2011	1161

Figure 2 complaints



Use of Statutory Enforcement Notices

The law provides our Office with an extensive "toolbox" to bring about compliance with the Data Protection Acts and the ePrivacy Regulations. We use these powers in a targeted manner. Our audit powers are covered below. We also have the power to order any action we consider appropriate in relation to the processing of personal data by a data controller and the power to require the production of information relevant to our investigations. Details of selected Enforcement Notices and Information Notices served by me in 2011 are set out in the following tables. I hope that publication of these lists encourages all organisations that are the subject of complaints to co-operate fully with my Office in relation to our statutory investigations. While I may issue an Enforcement Notice 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 my Office without the need for a formal legal notice to advance an investigation. Of course, where an organisation holds a different view as to the correct interpretation of the requirements of the Data Protection Acts, it is entirely appropriate for it to seek to appeal the issue of an Enforcement Notice to the Circuit Court.

Table 3 – Enforcement Notices * issued in 2011

Data Controller:	In relation to:
JP Distribution	Section 4(1) of the Data Protection Acts
The Clarence Hotel Sligo	Section 4(1) of the Data Protection Acts
Shandon Street Private Hospital	Section 4(1) of the Data Protection Acts
Gateway Transport Limited	Section 4(1) of the Data Protection Acts
Muster Developments Limited	Section 4(1) of the Data Protection Acts
Setanta Insurance Services Limited	Section 4(1) of the Data Protection Acts
Moonlite Cleaning Services Ltd	Section 4(1) of the Data Protection Acts
Highbird Limited(Irishcerts.ie)	Section 2(1)(c) and 2A(1)(a) of the Data Protection Acts
Births Deaths Marriages Limited	Section 2(1)(c) and 2A(1)(a) of the Data Protection Acts
Eircom Limited**	Sections 2(1)a, 2D, 2(1)(b), 2(1)(C)(ii), 2A(1), 2B, 2, and 2B(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.

** Under appeal to the Circuit Court.

Table 4 – Selected Information Notices* issued in 2011

Data Controller:
KC Civil Engineering Ltd
O'Brien & Co Insolvency Practitioners

*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.

Data Breach Notifications

The introduction of the data security breach Code of Practice in July 2010 has continued to have a marked effect on personal data security breach notifications to my Office. During 2011 my Office received 1167 data security breach notifications from

186 different organisations. This is a 300% increase in the numbers reported on in 2010 when we received 410 notifications. In 2009, before the introduction of the Code of Practice, the number of breach reports received by my Office was 119. As I stated in my Annual Report in 2010, I do not see this as an actual increase in the number of breaches occurring, rather a raised awareness of the need to notify my Office of a data security breach.

The coming into force of S.I. 336 of 2011 in July 2011, which gave effect to the revised *e*Privacy Directive, imposed mandatory reporting of data security breaches on all Telecommunication and Internet Service Providers. These data controllers are now required to notify my Office, without undue delay, of a data security breach. They are also required to notify individuals in all cases where there is a risk to their personal data.

75% of reported breaches related to errors in postal mailing (see Figure 3). In most cases, the breaches involved either multiple letters in the same envelope or a page relating to another individual incorrectly attached to a letter. These data security breaches are usually explained by human error. This shows that a large number of data security breaches could be prevented by simply taking a moment to examine documents prior to posting.

Another issue that caused me concern in 2011 were the reports made to my Office by the Health Service Executive (HSE) of inappropriate disposal of patient records. In one particular instance, my Office was notified of documents discovered in a litter bin outside of Roscommon General Hospital. Officials from my Office met with the individuals who discovered the documents and the documents were handed over to my Office. My Office then met with officials from the HSE to return the documents and demand an explanation of the matter. The HSE confirmed that the documents related to patients in Mullingar and it became apparent immediately from an examination of the documents that a doctor who had recently transferred from the Midlands Regional Hospital in Mullingar to Roscommon General Hospital was the most likely source of the breach.

This and a number of other similar breaches at the time caused me to write to the CEO of the HSE in the following terms referring to recommendations which I outlined in my Annual Report for 2009:

> "In light of recent developments I have no choice but to consider the use of my legal powers to compel the HSE to implement the recommendations listed above. Accordingly, please find attached a draft enforcement notice requiring that the HSE implements these recommendations. It is not valid until signed. In the absence of a personal response from you on these issues within fourteen days of the date of this letter, I will issue the enforcement notice without further notice or warning. It is an offence to fail or to refuse to comply with an enforcement notice without reasonable excuse. I wish to emphasise that I do not take such action lightly but am compelled to do so by the circumstances arising. I would also take this opportunity to note that the sequence of events which I have outlined demonstrate once again the lack of central responsibility regarding data protection matters within the HSE. The lack of clear policy leadership on data protection matters results directly in these types of repeated incidents but also prevents the HSE from adopting a strategic approach to data protection which would serve to enhance its capacity to deliver services to customers and patients through a modern information governance framework.
>
> I hope that the HSE finds itself in a position to respond positively on the requirements set out above and I look forward to the HSE's engagement in this regard."

I was heartened to receive a response from Mr. Cathal Magee within the period I had specified conveying his personal commitment to ensuring data protection requirements would be met in the HSE. Subsequently a National Director within the HSE was assigned lead responsibility in this area. While it is too early to assess whether this will result in the type of real engagement necessary which will benefit the HSE and individuals using HSE services, I was encouraged by the prominent

reference and understanding of the positive contribution which data protection compliance can make to the HSE on page 10 of its National Service Plan 2012.[7]

Table 5 – Number of Breach Notifications Received 2011

Total Number of Breach Notifications Received	1196
Number considered as non-breach	29
Number of Breach Notifications	1167

Table 6 – Number of Organisations making Breach Notifications

Private Sector Organisations	146
Public Sector Organisations	40

Table 7 – Breach Notifications – by Category

Category	Number
Theft of IT equipment	20
Website Security	37
Mailing breaches (postal)	870
Mailing breaches (electronic)	91
Security	34
Other	115
Total	1167

Table 8 – Comparison of Breach Notifications – by year

2009	60
2010	410
2011	1167

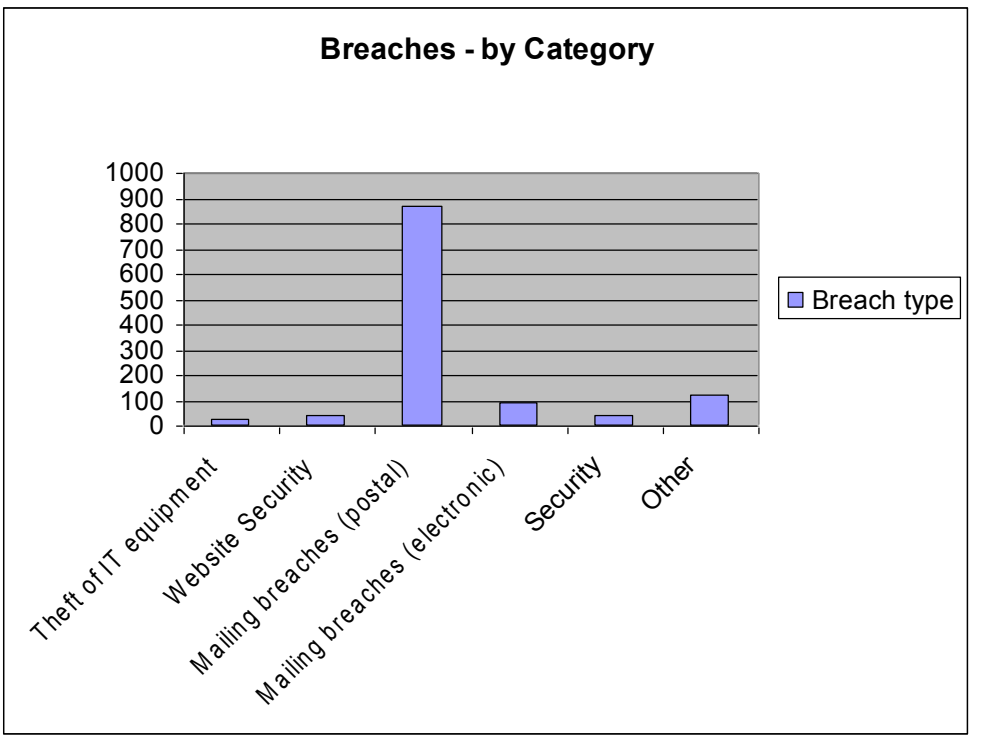
Table 9 – Comparison of Organisations making Breach Notifications – by year

Year	Private Sector	Public Sector	Total
2009	60	26	86

[7] http://www.hse.ie/eng/services/Publications/corporate/nspexecutivesummary2012.pdf

2010	89	34	123
2011	146	40	186

Figure 3 - Breach Notifications received 2011 – by Category



Theft of Revenue Laptops

The Office of the Revenue Commissioners notified this Office of the theft of 10 laptops from their premises on the evening of 27th January, 2011.

The laptops were encrypted, using modern encryption software with a complex password. The laptops had been chained to the desks. The thieves had forced their way through a fire exit and gained access to the offices in which the laptops were located. The laptops were later recovered by An Garda Síochána.

Our investigation of the matter confirmed that appropriate security measures were in place regarding the laptops but that physical security concerns needed to be addressed. As there was appropriate security measures in place on the laptops, this

Office considered that the data stored on the laptops was secure and that the Office of the Revenue Commissioners was not required to notify individuals whose data was stored on the laptops.

A physical security checklist was drawn up by the Office of the Revenue Commissioners and issued to building managers. This case shows the benefit of having properly secured laptops but also highlights the fact that security of personal data is not solely an issue of encrypting laptops or other equipment. The physical security of the data must also be considered.

Transposition of the ePrivacy Directive

On 1 July 2011 Ireland transposed the revised ePrivacy Directive by way of SI 336 of 2011. These Regulations revoked SI 535 of 2003 and SI 526 of 2008. I would like to thank the Department of Communications which closely consulted with my Office during the drafting and finalisation of the Regulations to ensure that we as the primary enforcement authority were clear as to the requirements of this new law. This close co-ordination also meant that the Office was in a position to publish Guidance on the new requirements on the same day as the law came into effect.

As outlined elsewhere in this report, the Regulations introduced a mandatory data breach notification requirement for electronic communications networks and providers. It also set a high bar for all such entities in relation to the security measures which they must take to protect personal data for which they are responsible. They must, inter alia, ensure that such personal data is secured and only available to approved personnel on a need to know basis. Failure to comply can result in a criminal prosecution with summary fines of up to €5,000 and on indictment €250,000 per offence.

The Regulations, despite their many other requirements, have become known as the "Cookie" Regulations as they introduced a requirement for websites to capture a consent from their users for the use of cookies. The scale of the consent, in our view, is relatable to the intrusiveness of the cookie. For instance there is a need to capture a specific consent in relation to so called behavioural advertising cookies which collect

information on websites visited by a user to allow for the provision of more targeted advertising as they surf the web. In other cases the provision of information on the home page of a site may go a long way to meeting the requirements. Our law specifically envisages that browser settings can be considered to provide a means of capturing consent. There is therefore a continuing opportunity for browser providers to assist in solving this problem.

My Office has approached the enforcement of these new requirements in a pragmatic way thus far. As this is now a well established law we are at the stage where we expect to see significant efforts made by websites to achieve compliance. We are mindful of industry initiatives to improve user knowledge and choice in relation to behavioural advertising but any website dropping or permitting cookies to be dropped or read will need to take some form of action now to meet its responsibilities. Failure to do so is not an option and will lead to action by my Office as required by the Regulations.

We also took the opportunity in the new law to clarify a number of matters in relation to direct marketing contact with consumers. Perhaps of most interest is that prior consent is now required to phone a person on their mobile phone for a marketing purpose unless that number is recorded as willing to receive marketing calls on the National Directory Database (NDD) – there are twelve such numbers so recorded as of 13 March 2012!

Also of interest is that a non-marketing SMS message may not have marketing material "tagged on" unless the recipient has given prior consent to the receipt of such messages. Also the requirements are extended to all forms of marketing carried out by means of a publicly available electronic communications service – including, for example, the soliciting of support for charitable organisations or political parties.

Other Enforcement Issues

General Election 2011

In my Annual Report 2009 I commented on the large number of complaints which I received from the public regarding unsolicited contacts by political parties or candidates for election in the course of the Local Government Elections. One of the issues of concern in 2009 was the manner in which candidates and political parties accessed personal contact details of voters. Conscious of the volume of complaints made to my Office in the context of the 2009 Local Government Elections, I wrote to all political parties in advance of the 2011 General Election to caution them about communicating with voters using SMS messages, emails or phone without consent.

I informed them that the Data Protection Acts cater for written communications with the electorate by providing that the restrictions on direct marketing do not apply to direct mailing carried out in the course of political activities by a political party or its members, or a candidate for elective political office. There was therefore no difficulty, for example, with the *Litir Um Thoghcáin* sent by candidates to individuals on the Register of Electors.

I pointed out that, during previous election campaigns, we received a substantial number of complaints from individuals in receipt of unsolicited SMS messages, emails and phone calls from political parties and candidates for election. In many cases, the individual had no previous contact with the political party or candidate and was concerned at how their details were sourced.

Unfortunately, it was necessary for my Office to commence twenty five separate investigations as a direct result of marketing by political parties and candidates in the course of General Election 2011. We also received in the region of seventy other complaints which it was possible to progress or conclude without having to open formal investigations.

A second issue of concern which I commented on in 2009 was the direct marketing exemption which excluded from the scope of the Data Protection Acts any direct marketing carried out for political purposes by political parties or by candidates for election to political office. I expressed my dissatisfaction then that I was unable to launch investigations into complaints which I received from voters who received unsolicited SMS messages, emails or phone calls even when they had made it clear that they did not wish to be contacted in that way. Had such unsolicited marketing contact been made to members of the public by any other entity, such as a commercial business, there would be no restriction on my investigating the matter. I expressed doubts in my 2009 Annual Report about the consistency with EU Directives of the exemption in this country for such political activities.

I am pleased to report that the Minister for Communications, in framing S.I. 336 of 2011, removed the exemption relating to direct marketing for political activities in the context of marketing communications carried out by electronic means – such as SMS messages, faxes, email and telephone calls. As a result, I am no longer restricted from investigating complaints in this area. Accordingly, in my role as Data Protection Commissioner, I am obliged to investigate any such complaints in this area. In this respect, arising out of the Presidential Election which took place following the commencement of SI 336 of 2011 on 1 July, I have already issued a warning to a political party about the sending of unsolicited marketing text messages in the course of the campaign. A second such incident is likely to lead to a prosecution.

Securing Mobile Phone Voicemail boxes

Revelations from the UK regarding phone hacking were covered extensively in the media in the summer of 2011. The general public was rightly concerned about the privacy of their voicemail messages (which was one aspect of the phone hacking revelations) as a result of the disturbing stories which emerged. In an attempt to protect, insofar as possible, the voicemail messages of subscribers in Ireland from suffering from similar hacking incidents, my Office commenced an engagement with the mobile network operators in Ireland. One of the issues which was clearly highlighted by events in the UK was the vulnerability of voice mailboxes on mobile

phones where the subscribers had not protected those mailboxes by using the facility to change the default password.

During our engagement with the mobile network operators, we established that the voicemail security features of some of the operators was better than others. However, all of the operators responded positively to our request to urgently examine customer voicemail security with a view to better protecting the personal data of their customers. Further to our engagement with the operators, they implemented a number of steps to enhance customer security and I am now satisfied that the security vulnerabilities that existed have been addressed.

Privacy audits

I am empowered to carry out privacy audits and inspections to ensure compliance with the law 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. These audits are in addition to investigations carried out by my Office in response to specific complaints. My Office also continued to conduct, where circumstances warranted it, unscheduled inspections of data controllers using powers conferred under section 24 of the Data Protection Acts and Regulation 19 of SI336 of 2011.

In the course of 2011, 28 audits in total were carried out by my Office. The number of audits in 2011 would actually have increased dramatically were it not for the fact that I conducted several major audits that were on a scale of engagement not experienced by my Office before. The asylum and immigration sector audits detailed below entailed visits of at least five days duration - the equivalent of five standard audits. I have already referred in my introduction to the scale of resources necessary for the Facebook-Ireland audit.

I believe an audit should be viewed as an aid to the organisation concerned in ensuring that its data processing operations are conducted in compliance with the provisions of the Act. For example, I randomly selected one particular sporting organisation for audit in 2011 so that I could examine garda vetting procedures in

place for adults working with juveniles. Initially, the organisation approached the audit process with a degree of trepidation but having reached the final report stage of the process thanked my Office *"for making a perceived daunting experience one we would recommend to others. We value your recommendations, input and assistance."*

My 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. Data controllers have demonstrated a willingness to put procedures in place to ensure they are meeting their data protection responsibilities in full. I would like to thank all of the organisations audited and inspected throughout the year for their cooperation.

Audit of Facebook Ireland

On 21 December 2011 we published the outcome of our audit of Facebook Ireland (FB-I) which was conducted over the previous three months including on-site in Facebook Ireland's Headquarters in Dublin. The Report is a comprehensive assessment of Facebook Ireland's compliance with Irish Data Protection law and by extension EU law in this area. As I said at the time, it was a challenging engagement both for my Office and for Facebook Ireland. The audit found a positive approach and commitment on the part of FB-I to respecting the privacy rights of its users. Arising from the audit, FB-I agreed to a wide range of "best practice" improvements to be implemented over the first 6 months of 2012, with a formal review of progress to take place in July 2012.

The Audit was the most comprehensive and detailed ever undertaken by our Office and placed a significant burden on the resources of my Office. My Deputy Commissioner worked almost exclusively on the audit for 3 months and was supported by a number of other staff members in our Office who had to equally commit a large amount of their time. As is well known we were indebted to UCD for providing to us, Dave O'Reilly on a pro bono basis. Without this support the audit outcome would have suffered greatly. This commitment on our part has continued into 2012 as we have continued to interact with Facebook Ireland on the commitments

given in the audit to ensure that these are met in a timely fashion. We have also communicated extensively with colleagues in other European data protection authorities and beyond on the outcome given our jurisdiction for Facebook Ireland's activities for users outside the US and Canada.

INFOSYS investigation

Also included in the list of the audits is an INFOSYS investigation. This refers to an in-depth examination of the use of INFOSYS – a database of social welfare data administered by the Department of Social Protection. The INFOSYS investigation focused on the authorised use of INFOSYS by a whole range of external third parties, including local authorities and state agencies. Initially INFOSYS was a 'desk audit' entailing extensive correspondence in the second and third quarter of 2011 between my Office and external users of INFOSYS. It was my intention to comment extensively on this investigation in this report but this has not proven possible, given the resources needed, to complete it to a suitable level. However, the interim findings have caused my Office to engage with the Department of Social Protection and the large number of entities authorised to access the system to address the deficiencies identified so far.

Finally, I issued An Garda Síochána with a letter of intention to audit them in 2011 but, owing to resource constraints linked to the Facebook audit and associated deadlines, I confined my engagement with An Garda Síochána in 2011 to two pre-audit meetings. The actual inspection of An Garda Síochána operations across a wide variety of platforms is now scheduled to take place in 2012.

List of Organisations Audited/Inspected

Athletics Ireland
Irish Life Assurance
Irish Naturalisation & Immigration Service (INIS)*
Garda National Immigration Bureau (GNIB)*
Dunmurray Springs Golf Club
Dublin GAA County Board
Recruitsafe

Birr Credit Union

Offaly County Council*

INFOSYS*

National Recruitment Federation (NRF) Garda Vetting service

Sarsfields GAA Club, Newbridge, Co. Kildare

Facebook Ireland

Nurse on Call

TP Robinson, Solicitors

Moloney & Co., Solicitors

Brian Lynch & Associates, Solicitors

Cabot Financial (Ireland) Ltd.

AIB Finance & Leasing

Bank of Ireland

Lothsdale Investments Ltd.

Grand Lodge of A.F. & A. Masons of Ireland (issue specific)

Xtravision, Tullamore (issue specific)

St. Joseph's College, Borrisoleigh (issue specific)

GlaxoSmithKline Pharmaceuticals, Dublin 16 (issue specific)

Midlands Prison, Portlaoise (issue specific)

HSE South, St. Stephen's Hospital, Glanmire, Co. Cork (issue specific)

Sacred Heart Adoption Society, Bessboro, Blackrock, Cork (issue specific)

* Not fully completed at end 2011

Policy issues

Vetting Bill

The views of my Office were sought on this very significant Bill prior to its publication. Last year I reported on guidance which my Office produced on the data protection considerations that arise from the conduct of vetting at present in this jurisdiction. The purpose of the guidance was to seek to ensure that vetting, which is necessarily intrusive by nature, does not expose persons who have consented to the

process to having their details disclosed beyond the organisation that is carrying out the vetting with the Garda Vetting Office. The legislation brought forward by the Department of Justice and Equality is seeking to also reflect that balance to ensure that those persons working or volunteering with children, vulnerable adults or in security sensitive positions are vetted but in a controlled manner that takes account of their right to privacy.

Guthrie Cards/Heel Prick Samples

This issue became the subject of public discussion during 2011 and into the start of 2012. The Newborn Bloodspot (heel-prick) screening test helps identify babies who may have rare but serious conditions. This Office first became aware of the retention of the heel prick blood samples and database in Temple Street in December 2009 on foot of revelations in the Sunday Times newspaper and the receipt of complaints from concerned parents who expressed shock that the samples of their children continued to be held and accessed in Temple Street.

We commenced a statutory investigation under the provisions of the Data Protection Acts. From the outset we engaged with the Department of Health and the HSE to identify an approach to this issue that brought the holding of the database back into compliance with the law. A deliberative and considered approach was adopted to ensure that the outcome reflected an appropriate balance between data protection law and legitimate health requirements. After over a year of engagement an agreed approach was arrived at in early 2011.

As a first principle, that agreement provided for enhanced information and choice for parents at the time of the heel prick test so that they understand at a basic level the purpose of the heel prick test and the use that is made of the samples. No such information was available to parents until then. This was introduced in July 2011. The agreement also provided for the destruction of all cards going forward after 11 years and the destruction of all cards held for over 11 years during 2011. The eleven year period which was suggested by the HSE and accepted by my Office is designed to deal with any requirement for re-testing of samples which arises from time to time and represents international best practice.

As part of the agreement reached, an information campaign is to be conducted that will provide choice to any parents who wish to have their child's card/sample destroyed where it is less than 11 years. Equally, in response to concerns expressed by groups such as SADS (Sudden Adult Death Syndrome), families will also be able to request that cards relating to them be retained where they were scheduled for destruction. This was in response to concerns around the need to access samples in relation to sudden adult death victims for the benefit of their families.

The SADS-related issue was not raised prior to the early part of 2011 nor did any access take place previously for such a purpose. The issue here was that in many cases blood samples were not taken from such victims after death. This will be resolved now by the putting in place of procedures to take such samples in future in this jurisdiction. This effectively fully resolves the issue identified and we understand that the HSE engaged with representative groups in this area to seek to fully address their concerns.

A final issue that emerged can essentially be summarised as that it would be useful to continue to hold the millions of samples involved to form the basis of a national database which could be used for health-related genetic (DNA) analysis We were obliged to point out that the creation of such a database, without the consent of the persons involved (or their parents/guardians as appropriate) would be a clear breach of the Data Protection Acts. It would also run counter to the spirit (if not the letter) of the Disability Act 2005 – which requires individual consent for the carrying out of genetic tests – and of the *Marper* judgment of the European Court of Human Rights in relation to the retention of DNA samples in a criminal context However, in light of concerns expressed around such issues, we understand that the Minister for Health asked for a full review of the decision taken by the HSE to destroy the samples on the terms agreed with this Office. We were not a party to this review but it is now completed and at the time of writing the Minister had approved the position previously agreed including the publicity campaign for people to seek earlier deletion or continued retention depending on their own particular preferences.

The position of this Office is that we will be closing our investigation of this issue

once the agreed approach is fully implemented. However, it is important to make clear that the position that developed was unlawful and could not be allowed to continue. Failure on the part of this Office to act could have led to a valid complaint that we had not correctly met our supervisory obligations and as a consequence the requirements of European law in this area and could have led to action against Ireland.

Insurance Link

In my Annual Report for 2010, details of our investigation into the use of 'Insurance Link' by the insurance sector were extensively outlined. One of the key recommendations which emerged from this investigation was that detailed personal information held by an organisation relating to a previous claim should only be released to another insurance company on foot of a court order or with the explicit consent of the individual concerned. We did indicate at that time, however, that we were open to exploring other legal avenues that might be available for such disclosures to take place in conjunction with the putting in place of formalised protocols governing any exchanges.

During 2011, we continued to engage with the Irish Insurance Federation (IIF) and the Self Insured Task Force on behalf of their respective members to review proposals from the industry to put in place a formal structure for the exchange of agreed categories of information in relation to previous claims. Given the lack of formal and standardised procedures which had operated within this sector, we welcome the ongoing commitment to developing processes in compliance with the Data Protection Acts and we look forward to finalising an agreed approach for exchanging data which can be fully justified from a data protection perspective.

Engagement with National Board for Safeguarding Children in the Catholic Church

My Office continued its engagement with the National Board for Safeguarding Children in the Catholic Church and other Church Bodies during 2011. The National

Board for Safeguarding Children was established by the Church Bodies in 2006. Its remit is to advise its three sponsoring bodies (the Irish Bishops Conference, the Conference of Religious in Ireland and the Irish Missionary Union) on best practice relating to child protection policies and procedures. The Board also develops policies and procedures to guide all constituent members of the Church in relation to best practice in safeguarding children. Another function of the Board and the matter on which the further advice of the Office was again sought during 2011 relates to the monitoring of practices in the various parts of the Church, through processes of audit and review.

During our initial engagement, we agreed a data-protection-compliant mechanism to allow the Board to carry out its audit functions and we were advised that this mechanism has worked well and that the specific auditing objectives of the Board were being met. During 2011, our assistance was sought in relation to follow on reporting procedures which the Board wanted to put in place with the Church bodies to further ensure best practice with respect to child protection matters.

I believe that this latest engagement builds upon what has been a positive and productive engagement to date and the agreed approach takes due account of the sensitive nature of the data involved as well as the complex data protection as well as other legal considerations which must be examined in relation to the handling of personal data in this area.

Department of Finance Credit History Working Group

My Office participated in an Inter-Agency Group on Credit Histories established by the Department of Finance in December 2010 following a commitment made by the then Minister for Finance. It was established to (a) examine the extent to which the current national credit reporting system was fit for purpose and (b) to make recommendations, as necessary to rectify any system weaknesses having regard to the terms of reference of the Group. The Group included officials from the Department of Finance, the Department of Jobs, Enterprise and Innovation, the Central Bank of Ireland, the Competition Authority and representatives from my Office. The Group

met on 12 occasions from January 2011 until it concluded its deliberations in June 2011.

The Terms of Reference of the Group were as follows:
"To develop a strategy to put in place an effective credit reporting system in Ireland that will support:

- Informed lending decisions
- Supervisory activity of financial institutions including prudential supervision
- Consumer protection
- Competition in credit markets
- Economic development
- Wider branches of the State

Cognisance will be taken of the work of the Central Bank of Ireland in regard to the credit reporting system and of its recommendations in this regard"

The Group engaged in a wide consultation process before finalising its report which contained a number of key findings and recommendations which if implemented will see a number of fundamental changes to the way the credit reporting system operates in Ireland. The full report of the Working Group was submitted to the Minister for Finance in July 2011 and the Department of Finance has been working on developing legislative proposals in this area in line with Ireland's commitment under the EU/IMF Programme of Financial Support for Ireland.

This Office was invited to participate in the Working Group given its regulatory role in respect of the use of personal data by credit reference agencies and credit information services. The Data Protection Act provides individuals with important rights to ensure that their data are accurate and are used appropriately. However, for individuals to be in a position to exercise these rights effectively, they naturally need to be conscious of the degree to which their personal data are being kept, and to have some practical understanding of how the credit referencing system operates currently. It was on this basis that my Office enthusiastically participated in the work of the Group. I am hopeful that the final outcome, that will be reflected in legislation, will

take account of the balance that must be struck in this area between the need for quality and reliable credit history information to inform lending decisions and the need to only seek relevant and necessary information without unnecessarily infringing borrowers reasonable right to privacy.

Integrating Ticketing System

The roll out of an 'Integrating Ticketing System' for public transport users in Dublin commenced in 2011. The new *'Leap'* card is a smart card containing an electronic chip which allows members of the public to use Dublin Bus, Luas, Dart and rail services using one ticket.

My Office was consulted by the Railway Procurement Authority and the National Roads Authority from the very initial stages of the project in order to ensure the sharing of data between different transport operators was handled in a manner compliant with data protection legislation. My primary consideration was to ensure key safeguards were in place from the outset in relation to the processing of customer registration information and journey data.

Significantly, it was agreed during the project design stage, that the integrated ticketing scheme would not carry, retain or process data that identified departure or arrival locations. Transaction records would only detail the specific transport operator in question, the cost of the journey, the date and approximate time. The retention of journey data and the length for which it is kept by transport authorities has often raised concerns amongst privacy activists worldwide and so I welcome the approach taken by the transport operators here in Ireland.

Leap cards can also be purchased anonymously. This is an important option to offer customers from a privacy perspective. Registered cards can also be purchased, which offer the user the reassurance if their card is reported lost or stolen that they will be refunded the credit on the card and no one else can use it. I am aware that registered cards entail the capture of personal data about the purchaser but this information is not stored on the chip on the card. In addition, there are personalised cards on offer such as TaxSaver tickets which are cards that can only be issued to a specific, named and

authenticated individual. Again, it is important to note that any additional information gathered is not stored on the chip on the leap card, other than a flag identifying that the card in question is a personalised card.

I wish to thank all those involved in the Integrated Ticketing Scheme project for consulting with my Office from the outset. I wish continued success to the project as other transport operators come on board. I look forward to providing assistance with future projects, including the proposed link-up with the integrated Ticketing Scheme and the Public Services Card in terms of travel cards for the over 65s.

Eurobarometer Study

A Eurobarometer Report entitled '**Attitudes on Data Protection and Electronic Identity in the EU'** was published in June 2011. The survey was commissioned by the European Commission and conducted by TNS Opinion & Social, a company based in Brussels.

The report[8] presents the results of the largest survey ever conducted regarding European citizen's behaviours and attitudes concerning identity management, data protection and privacy with a special focus on the Internet. More specifically, the report addresses Europeans' actual disclosure of personal information, their awareness of and perceived control over their personal data, their ways of protecting personal data, and the data protection regulatory environment they would like to see.

26,574 Europeans aged 15 and over across the 27 EU member states were interviewed in total, including 975 individuals who were interviewed in Ireland.

What is Personal Data?

- A key question asked was what types of data would be considered to be 'personal data'. The results show 93% of Irish respondents to the survey classifying medical information as personal data, followed by financial information at 89%, with national identity card/numbers and fingerprints at 85% and 81% respectively.

[8] http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Approval to Process Personal Data

- All respondents to the survey were asked whether their specific approval should be required before any kind of personal information is collected and processed. A country-by-country analysis reveals that respondents in Greece and Cyprus (each 98%), the Czech Republic (97%), and Ireland, Malta, Slovakia, and Bulgaria (all 96%) are most likely to say that their specific approval should be obtained.

Social Networking

Overall, the survey found that of the 27 member states, social networking sites are used most often in Hungary (80%), Latvia (73%), Malta (71%), followed by Ireland (68%). Social networking sites were used least in Germany (37%).

In terms of privacy settings:

- 54% of Irish respondents indicated they had tried to change the default privacy settings of their personal profile on a social networking site, with 88% of those who had done so deeming it "easy" to make these changes.

In terms of transparency:

- 65% of Irish social network users indicated they considered they were informed about the conditions for the collection and further use of their data when asked to disclose personal information in the course of becoming a member of a social networking site or registering for a service online.

- 60% of respondents indicated they felt sufficiently informed by social networking sites about the possible consequences of disclosing personal information.

Respondents who use social networking or sharing sites were asked who they think should make sure that their information is collected, stored and exchanged safely on these sites. A country-by-country analysis shows that in 23 of the 27 EU Member States, respondents primarily hold themselves responsible for the safe handling of

personal data, most strikingly in Cyprus (68%), **Ireland** and Romania (both 65%), and Malta (64%); the lowest scores were recorded in Spain (37%) and Italy (38%).

I believe this is evidence that users of social networking sites in Ireland understand that, as well as the data protection obligations placed on social networking sites, individual users must exercise personal responsibility regarding the data they post online about themselves and others.

Public Services Card

The rollout of the new Public Services Card by the Department of Social Protection commenced in 2011, with the card introduced on a phased basis to approximately 5,000 social welfare recipients across the country. I welcome the incremental nature of the roll-out of the Public Services Card as this allows the Department to monitor its implementation and iron out any potential issues that might arise in advance of the card being distributed on a universal basis.

In 2011, my Office visited the Public Services Card personalization and distribution facility accompanied by officers from the Department of Social Protection and were satisfied on the basis of their tour of the facility that there is a strong security focus in evidence throughout the backend operation.

My key concerns in relation to the Public Services Card have always been based on the potential for 'function creep' with regard to the proliferation of the PPSN and the potential risk that it will be seen as a de facto national identification card.

I will continue to follow all developments associated with the public services card very closely to ensure it is used in an appropriate manner and does not give rise to any data protection or identity theft concerns.

Association of Compliance Officers in Ireland

Effective implementation of data protection at the level of individual organisations must include assignment of day-to-day responsibility for compliance to a specific

individual or unit. As regulatory compliance has become more demanding in general, there has been increasing recognition that a specific set of skills is required to perform the task effectively. The Association of Compliance Officers in Ireland (ACOI) has done much to develop the skill-set required among its members. We have been happy to assist it wherever possible.

In October, the Association published a "Data Protection Regulatory Guide" which explains, in practical language, how the principles of data protection apply in an organisational setting. The Guide is a very useful resource for members of the Association in ensuring a high level of compliance with data protection law

"Cloud" Computing

As reported in our 2010 Report, "Cloud" computing - in essence the transfer of data to a data centre where a "cloud" provider provides varying degrees of data processing – is increasingly being adopted by businesses as a more cost-effective and flexible model for the processing of their data. Many of the major "cloud" providers have established data centres in Ireland. The main issues for data protection are the respective responsibilities of the "cloud" provider and its clients and the additional responsibilities that apply where data is being transferred outside of Europe.

In June, the Minister for Jobs, Enterprise and Innovation established a group to consider the potential for further developing the potential of "cloud" computing in Ireland. We participated in the work of the group, which is expected to report to Government in 2012.

EU & International Responsibilities

Intel 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" (BCRs). BCRs 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 order to secure approval for BCRs, 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. This approval receives mutual recognition from a number of other data protection authorities across the EU.

In late 2010, we took on the role of lead authority in respect of Intel Corporation's BCR application. This intensive review of Intel's Corporate Privacy Rules continued throughout 2011 in conjunction with other relevant EU Data Protection Authorities and was completed in January 2012[9]. The approval process for Intel's BCR was led by my Office due to the location of Intel's European Manufacturing Centre in Ireland which is Intel Corporation's single biggest location in Europe. BCRs are a valuable tool for corporations that recognise the corporate benefit in striving to embed privacy principles into their business practices on a daily basis and to comply with EU data protection requirements. I would like to thank Intel Corporation for the positive engagement throughout the approval process in 2011 and look forward to continuing to work with them.

Article 29 Working Party

The Article 29 Working Party acts as an adviser to the EU Commission on data protection issues. It also promotes a uniform application of the provisions of the EU Data Protection Directive 95/46/EC throughout the European Economic Area.

In the course of 2011, the Working Party continued to give close attention to issues relevant to the future EU data protection regime, taking account of the European Commission's Communication of November 2010. It produced Opinions on the

[9] http://dataprotection.ie/viewdoc.asp?DocID=1190&m=f

circumstances in which processing of personal data can take place on the basis of individual consent and on the issue of the reporting of data breaches to individuals and to data protection authorities.

The Working Party also gave its views on: data protection issues related to money-laundering and terrorist financing; geolocation services on smart mobile devices; 'smart' metering; use of passenger data for the investigation etc of offences; a privacy impact assessment framework for RFID applications; online behavioural advertising; and the data protection system in New Zealand which it considered guarantees an adequate level of protection for personal data.

The Working Party also laid the groundwork for an expanded role in the area of police and judicial cooperation, in the light of the changes brought about by the Lisbon Treaty.

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

Data Protection in EU Specialised Bodies

The Office continued to be represented – at a minimal level due to resource constraints - at meetings of the data protection bodies overseeing activities in specialised EU bodies. These include 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 (which ensures that personal data within the European Customs Information System is processed in a manner that respects data protection rights) 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 32nd International Conference of Data Protection and Privacy Commissioners hosted by our colleagues in Mexico.

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 contributed to a "twinning" project between the Spanish Data Protection Agency and the Data Protection Authority of Croatia.

We continued to participate in the "accountability" project during 2011. The project is led by the US-based Centre for Information Policy Leadership. It explores what an organisation needs to do to demonstrate that it can be trusted to handle personal data responsibly. In 2011 the project moved to a third phase – facilitated by the Spanish Data Protection Authority – focussed on implementing accountability. A Discussion Paper on this aspect was published in November.

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 2011 were as follows:

	2010 €	**2011 €**
Overall running costs	**1,449,329**	**1,523,620**
Receipts	**629,668**	**592,710**

A fuller account of income and expenditure in 2011 is provided in Appendix 3.

Part 2

Case Studies

Case study 1: Leisure centre requests excessive personal data from patrons.

In October 2010 I received a complaint from an individual in relation to a leisure centre, Swan Leisure in Rathmines, refusing him and his child entry to its swimming pool because he declined to complete its Guest Registration Form. The complainant provided a copy of the Guest Registration Form. The first page of the form requested details such as the individual's name, address, date of birth, email and mobile phone number. The second page consisted of a list of medical-related questions such as the person's family medical history of heart disease, respiratory disease and diabetes, the extent to which they may be overweight, and details of their lifestyle. The complainant refused to complete the registration form because he considered it to be too intrusive as it required him to divulge sensitive, personal medical information. He said that he should be able to take his child for a swim without having to provide sensitive personal information.

Section 2(1)(c) of the Data Protection Acts, 1988 and 2003 provides that data "shall be adequate, relevant and not excessive" in relation to the purpose for which it is kept. My Office informed Swan Leisure that we considered its practice of requesting the aforementioned information to be excessive. In addition we pointed out that medical data is deemed to be sensitive personal data and its processing is subject to additional safeguards under the Acts. We asked the leisure centre to outline to us the basis on which medical data was sought and how the processing of that information complied with its obligations under the Acts.

In its reasoning for asking guests who attend the facility to provide their name and contact information, Swan Leisure referred to its Child Protection Policy. It indicated that in order to safeguard children attending its facilities it was imperative that it take a record of everyone that came onto the premises. It was not clear to us how having the name and address of every person attending the facility was relevant to child protection. In relation to the medical screening forms, the leisure centre informed us that the reason for requesting guests' medical data was to help prevent injuries or medical issues arising from the use of its facilities. It also referred to advice given by the American College of Sports Medicine (1976) stating that anyone who has risk

factors for heart disease (a family history of heart disease, a history of smoking, high blood pressure or high blood fat levels) should be given a full medical examination before exercising in a health club. The leisure centre informed us that it was collecting medical information under Section 2(B)1 of the Acts which, among other things, allows the processing of sensitive personal data where the processing is necessary to prevent injury or other damage to the health of the data subject or another person.

Having reviewed its response, we told Swan Leisure that its policy of recording the name, contact details and medical information of all of its patrons was unacceptable. We acknowledged the importance of protecting children and safeguarding the health and well-being of patrons during the use of the leisure facilities. However, we informed it that from a data protection perspective, the systematic recording of patrons' information was a disproportionate response to the aims it sought to further, i.e. health promotion and the protection of children. We further informed the leisure centre that the request for such information could not be justified by reference to the policy guidelines and academic commentary it had cited.

In its response, the Centre referred to the Institute of Leisure and Amenity Management (ILAM) facility standards. Following further communications with my Office, the leisure centre subsequently confirmed that in order for it to meet both ILAM's guidelines and the Data Protection Guidelines it had changed its policy so that it now offers a guest register form. However, the completion of this form is no longer a condition of entry to the leisure centre and the right of patrons not to provide the personal information requested is respected. In relation to the forms already completed prior to the introduction of this change, it informed us that guests would be given the option to have their data deleted at any point during or after their time with the centre. As a result of this complaint, members of the public may now use the swimming pool at the leisure centre on an anonymous basis and that is as it should be.

Case Study 2: Telecommunications companies prosecuted for marketing offences.

Arising from a number of complaints which I received in 2009 and 2010 I took prosecution proceedings against four telecommunications companies in March 2011 in relation to offences under SI 535 of 2003 (as amended). The cases against Eircom, Vodafone, O2 and UPC were heard on the same day at the Dublin Metropolitan District Court.

Eircom

Eircom entered a guilty plea in respect of one charge for an offence under Regulation 13(4)(b). The charge related to an unsolicited marketing telephone call to an individual whose landline number stood recorded on the NDD opt out register as not wishing to receive marketing calls. During the course of our investigation of this complaint, we established that the call had been made from a mobile phone used by one of the company's "feet on the street" sales agents. The list used by the agent had not been cleansed against the NDD opt out register. The Court accepted the guilty plea and it applied the Probation of Offenders Act conditional upon a payment of €2,000 being made by Eircom to Accord.

Vodafone

Vodafone entered guilty pleas in respect of four charges under Regulation 13(4)(b) and one charge under Regulation 13(1)(b). The charges under Regulation 13(4)(b) related to the making of repeated unsolicited marketing phone calls to an individual whose landline number stood recorded on the NDD opt out register. The calls were made between September 2009 and June 2010. Three of the four calls were made while my Office's investigation was ongoing. The Court accepted the guilty pleas, it entered convictions against Vodafone in respect of all four charges. It imposed a fine of €250 in respect of the first unsolicited call, €400 in respect of the second call, €1,000 in respect of the third call and €1,200 in respect of the fourth call.

The charge under Regulation 13(1)(b) related to the sending of an unsolicited marketing text message in February 2010 to a customer who had opted out of receiving marketing communications from Vodafone. The customer had complained previously to my Office in 2009 about the sending of such marketing text messages by Vodafone. Further to that complaint the company assured us that it had opted her out of further marketing contact. The Court accepted the guilty plea, it entered a conviction against Vodafone and it imposed a fine of €1,000.

O2

O2 entered a guilty plea in respect of one charge under Regulation 13(1)(b). The charge related to an unsolicited marketing text message sent to a customer in February 2010. The customer had previously opted out of receiving marketing communications from O2 in 2007. The Court accepted the guilty plea and it applied the Probation of Offenders Act conditional upon a payment of €2,000 being made by O2 to The Spinal Injuries Fund.

UPC

Guilty pleas were entered by UPC in relation to eighteen charges against it under Regulation 13(4)(a). The charges related to the making of unsolicited marketing phone calls to four individuals who had previously informed UPC that they did not wish to receive further marketing calls. In one case the defendant faced twelve charges for persistent calling of an individual in a two-week period in 2009. The Court recorded twelve convictions in this case and it imposed fines of €400 for each conviction. In the second case, UPC was convicted on three charges of making unsolicited marketing phone calls and the Court imposed a fine of €300 on each conviction. In the third case, two convictions were recorded with fines of €400 imposed for each. In the last case, one conviction was recorded with a fine of €600 imposed by the Court.

The total amount of fines imposed on UPC amounted to €7,100. In deciding the penalties, the Court noted that UPC had two previous convictions arising from

prosecution proceedings taken by me in 2010 concerning the making of unsolicited marketing phone calls.

In all of the above cases, the defendants paid costs to my Office. I was very pleased with the outcome of the prosecution proceedings in these cases. It sent a strong message to organisations that they must comply with the law which applies to the making of unsolicited marketing contact with individuals, be they customers or not, or else risk prosecution and the consequences of a criminal record.

UPC Settlement

At the time of the prosecution proceedings against UPC, my Office had three complaints on hands concerning unsolicited marketing telephone calls, the investigation of which had not been completed. By mid-year those investigations were concluded and we were satisfied that prosecutable offences had been committed in respect of each complaint. We met with UPC to present it with the options (including prosecution) available to us to progress these files to a conclusion. Subsequently, we reached agreement with UPC in August 2011, the terms of which included a goodwill gesture of €500 to each of the three complainants, an overall donation of €20,000 to charity (this amount was shared among four Irish charities- Focus Ireland, Canteen Ireland, Respect and The Jack & Jill Children's Foundation) and the publication of a statement on the homepage of the UPC website. This statement, among other things, outlined broadly the terms of the agreement and it indicated that additional controls had been put in place internally and with third party sales agents to ensure that customer preferences are accurately recorded in future. The statement also noted that the Office of the Data Protection Commissioner was satisfied that UPC now has in place improved procedures to enable it to fully comply with its data protection obligations.

Case study 3: Prosecution of Regine Ltd for the sending of unsolicited marketing text messages.

In 2010 I received a complaint regarding marketing text messages sent by Regine Ltd, trading as Fran & Jane. The complainant stated that she had never consented to the receipt of marketing text messages from them. She informed me that she had phoned the Fran & Jane outlet in Clarendon Street, Dublin on numerous occasions to ask for her phone number to be removed but despite her requests she continued to receive marketing text messages. Furthermore, the text messages contained no opt-out mechanism.

In response to our investigation, Fran and Jane admitted that it had no opt-out facility in the message due to a lack of awareness about this requirement. It indicated that, in future, an opt-out would be included in all marketing text messages. Regarding its failure to respond to the opt-out requests made by telephone to its Clarendon Street outlet, it informed us that the database of customer contact details is controlled at its head office and that the outlet concerned had not passed on the opt-out requests. It apologised for these oversights. At this point, in May 2010, Fran & Jane informed us that the complainant's mobile phone number had now been removed from its marketing database. In line with our usual "two-strikes" policy on such matters we noted its assurances and we issued a formal warning.

The same complainant contacted us again in October 2010 to inform us that she had received a further marketing text message from Fran & Jane despite the previous assurances given to my Office. We contacted the company again and we were informed that due to human error it had removed a different but similar number from the database on the previous occasion. Fran & Jane then assured us in November 2010 that the complainant's phone number had been fully removed from its database.

While our investigation was ongoing, the complainant contacted us for a third time to inform us that she had received another marketing text message in December 2010 which did not include an opt-out facility. On seeking an explanation for this latest breach, Fran & Jane told us that its service provider for the marketing service was responsible. We subsequently received correspondence direct from the service

provider. This indicated that when the number was given to it by phone for the purpose of being opted out, it was initially entered on the stop list system as a fax number. This was noticed and it was altered to a mobile number on one platform. The alteration was not made on a second platform. This led to the number being targeted again on a further marketing campaign. It informed us that it had since corrected the error.

I decided to take prosecution proceedings in this case in light of the repeated offending behaviour. In June 2011 the case came before Dublin Metropolitan District Court where Regine Ltd, trading as Fran & Jane, pleaded guilty in respect of one offence under Regulation 13(1)(b) of SI 535 of 2003 (as amended) for the sending of a direct marketing text message without consent. The Court accepted the guilty plea, a conviction was recorded and a fine of €450 was imposed.

Case study 4: Marketing phone call made to a number on the National Directory Database (NDD) Opt out register.

I received a complaint regarding a marketing phone call made by a life assurance company Acorn Life Ltd. The complainant stated that her preference was recorded on the National Directory Database (NDD) Opt-Out Register not to receive marketing phone calls. On receipt of this complaint, we checked the complainant's phone number against the NDD Opt-Out register which showed the phone number had been opted out of marketing when the call was made.

In response to our investigation, Acorn Life Ltd stated that a member of its telesales team had made the marketing phone call to the complainant. It stated that its procedure was to clash a prospective number against the NDD Opt-Out Register to ensure that it was not listed. It could not confirm that this procedure was followed in this instance as the staff member who made the call had left the company in the meantime.

Acorn Life Ltd stated that it wished to apologise to the complainant and by way of amicably resolving this complaint it suggested a donation of €500 to a charity of the complainant's choice. The complainant accepted this offer. In addition, a formal warning was issued to Acorn Life Ltd to the effect that if we received any further complaints regarding its marketing operations prosecution action may be taken against it in the event that offences were found to be committed.

This case highlights the need for those involved in marketing activity to follow correct procedures to ensure that marketing calls are not made to those wishing not to receive them. The simple step of properly clashing the complainant's phone number against the NDD Opt-Out Register would have ensured that the number was not called in this instance and a breach would have been avoided.

Case study 5: Unlawful obtaining and use of email addresses for marketing purposes by The Zone Extreme Activity Centre.

I received a complaint regarding a marketing email sent by The Zone Extreme Activity Centre. The means by which the activity centre obtained the email address of the complainant as well as the email addresses of many other people was a matter of concern to my Office and is worthy of detailing in this case study as a lesson to those involved in marketing. The circumstances were as follows:

An entity previously received an email from a now defunct company which mistakenly included a list of recipient email addresses in the "To" field, rather than in the "BCC" field. That entity then forwarded on these email addresses to the activity centre with the message "I just found this email that (Name removed) sent me last Christmas and they stupidly had all the email addresses on their mailing list in the TO bar…. Guess there yours now……". The activity centre subsequently used the email addresses to send an unsolicited marketing email promoting a Christmas party at the centre. Included at the bottom of the marketing email was an email thread containing the full details of all of the email addresses. In the process of issuing the marketing email complete with the email thread, the activity centre then further disclosed this personal data, which included both personal and business email addresses, to everyone to whom the email was sent.

It was clear in this case that the personal data in the form of email addresses was not obtained fairly by the activity centre from the other entity. This was also abundantly clear to the activity centre given that the method of obtaining the messages was fully disclosed to it by the original email recipient. This personal data was then processed unlawfully by the activity centre in the sending of the marketing emails to the list of email addresses it had no consent to send marketing emails to in the first place. In addition, by supplying the email addresses to the activity centre without the consent of the individuals concerned, the other party also unlawfully processed the personal data.

In response to our investigation, The Zone Extreme Activity Centre stated that it was their intention to contact the businesses on the email list to ask if they would mind receiving a marketing email about the Christmas Party in the centre. It accepted that

the email should never have been sent out and that it had no authority to do so. My Office also wrote to the other party who had forwarded the list of email addresses to the activity centre. In its response, that party stated that it understood that the email list it forwarded would be cleaned and verified by the activity centre before any marketing emails were sent out. It stated that its intention when sending on the email list to the activity centre was a friendly one and it did not sell this list or pass it on to anyone else.

We insisted that any holdings of the email list in question by the activity centre and by the other party be destroyed. We issued a formal warning to the activity centre to the effect that if we received any further complaints regarding its marketing operations, prosecution action may be taken against it in the event that offences were found to be committed.

This case highlights a growing concern whereby businesses are sometimes careless in the way they handle bulk emails and expose the email addresses to all recipients. As can be seen from this case, an entity took advantage of an open email list and proceeded to use it for its own marketing purposes, clearly in contravention of the Regulations.

Case study 6: Customer data legitimately passed from car dealership to new buyer.

In November 2010 I received two complaints from individuals who had received direct marketing text messages from a car dealership promoting special offers. Both of the complainants had previously purchased cars from a firm which had since ceased trading. Since closure, some of the sales team had become involved with the new car dealership which was now the subject of the complaint to my Office. Neither complainant had consented to receiving direct marketing text messages from the new dealership.

As part of the investigation of these complaints, my Office contacted the new dealership to obtain details, if any, of the consent it had in place to send the text messages to the complainants. In its response, the dealership informed us that it had purchased the previous dealership from the liquidator and it had taken over the existing premises, staff, equipment, stock, etc. From this purchase it had obtained the full database of previous customers. The contact details of both complainants were contained within this database. As customers of the previous business, both complainants had opted in to receive marketing messages at the time of their car purchase and/or car service. The dealership confirmed that it had now unsubscribed both customers from their database so they would no longer receive any future marketing messages. It also offered an apology to both complainants for any confusion caused.

Where a company purchases a business from a liquidator, it is likely that in circumstances where the customer data is to be used by the purchaser for the same purposes as the previous owner had used them, there would not be a data protection concern. If the customer data was to be considered for use for another purpose then the liquidator would need to get an opt in consent from those customers on the database to pass on their personal information to the new buyer. In the above case the customer data was used for the same purpose as previously by the new buyer so no breach of the Data Protection Acts arose.

Case study 7: Allianz requesting excessive personal information at quotation stage.

In May 2011 I received a complaint from an individual in relation to what she considered to be the excessive level of personal information requested by Allianz when she contacted them by telephone seeking a pet insurance quotation.

The complainant informed us that during the call to Allianz the agent asked her to provide her date of birth and her mother's maiden name. The complainant informed the agent that she was not a policy holder with the company and that she was only seeking a quotation. The agent then informed the caller that it was a requirement under the Data Protection Acts, as a security measure, to ask such questions.

Our communications with Allianz concerned two issues, the first one being the use of information from a birth certificate as a security question. Allianz informed us that it introduced three ID security questions consisting of date of birth, mother's maiden name and place of birth. It stated that these questions were introduced to ensure that it was keeping its customer's personal information safe and secure and to prevent any unauthorised disclosure. As previously outlined in my 2009 Annual Report it is our view that the use of questions such as date of birth and mother's maiden name for the purpose of ensuring security of data is not an adequate safeguard against disclosure to a third party. Such questions may in fact be a security vulnerability as this type of information is publicly available upon payment of a fee to the General Register Office and is therefore of limited value on its own as a security feature.

The second issue concerned excessive data collection in the context of a quotation. We informed Allianz that there was no requirement under the Data Protection Acts for it to collect date of birth, mother's maiden name and place of birth data when a person phones for a quotation – especially for pet insurance! The Acts provide that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or are further processed. We told Allianz that to suggest to a person who phones for the first time to seek a quotation for insurance that the collection of such information is a requirement under the Acts was both false and misleading and was a misrepresentation of the requirements of the Acts. When

queried, Allianz confirmed to my Office that a quote reference number is provided over the phone so that a customer could note it for further reference. It also confirmed that unless the caller indicated that the quote was, for example, too expensive or that they were no longer interested, a quote pack would usually issue to the customer containing a quote reference number. It was our view that confirmation by a caller of the quote reference number in a follow up call would adequately meet any data security requirements the company may have at quotation stage.

Following our intervention, Allianz confirmed its intention to cease using its ID verification screen at quotation stage. In future, it undertook to not seek information at quotation stage regarding a caller's date of birth, mother's maiden name and place of birth.

The use of ID verification questions is common practice among companies in order to ensure the safety and security of personal data of their customers or policyholders and to prevent against unauthorised disclosure. This is a practice which we of course encourage in relation to the protection of customer personal data in appropriate circumstances. However, verification of a caller's identity can be easily achieved without asking questions that are bordering on invasive or which might cause upset to the caller. In addition, we discourage the collection of unnecessary personal data at quotation stage, such as in the case outlined above in relation to pet insurance. If the caller decides, having obtained the quotation, to take out a policy, it would be acceptable then to seek personal data which might be used for ID verification on subsequent calls concerning the policy.

Case study 8: Veterinary practice discloses dog owner's personal data.

In October 2010 I received a complaint from an individual who alleged that a veterinary practice had disclosed her personal information, i.e. her name and address details, to a third party, namely the original owner of a stray dog that she was now in possession of. In her complaint she explained that when the dog was found its original owner had been contacted using the information logged in connection with its identity microchip and that he had indicated that he did not want the dog returned. Following this, she said that the microchip and ownership details of the dog transferred to her. She indicated that all of these matters were conducted by her local vet (who was not the subject of this complaint). The complainant stated that she subsequently received a letter addressed to her at her home address from the dog's original owner. This letter included a request by the previous owner to meet with her and the dog and it enclosed records of the dog's medical history as compiled by the previous veterinary practice which the dog had attended. The complainant alleged that the previous veterinary practice had breached her data protection rights by disclosing her name and address to the original owner of the dog.

This matter was investigated with the veterinary practice complained of and we sought an explanation for the alleged disclosure of personal data. The veterinary practice acknowledged that it had searched for the new owner's contact details and had given them to the previous owner. This arose when the previous owner told the practice that he had re-homed the dog, that he wanted to check to see if the new owner had re-registered the microchip in their own name and to ensure that it was no longer registered in his name. The veterinary practice took this to be a reasonable request and it accepted its bona fides. On being notified of our investigation, the veterinary practice realised that the original owner had misrepresented the purpose of his request for information. The new owner's details were not held on the database of the veterinary practice concerned as she was not their client. Instead, the veterinary practice carried out a search using the dog's microchip number on the website www.fido.ie - which is a database of microchipped pets to which veterinary surgeons have access. Having found on the website that the dog's microchip was no longer registered to the previous owner, the veterinary practice informed the previous owner

accordingly and, in that context, it also disclosed the name and address of the new owner.

The veterinary practice said that it was sorry if its actions had created a situation which caused upset to the complainant and stated that it would not have happened had it been advised truthfully of the situation. It stated that as a result of this complaint all staff at the practice are now thoroughly aware of the need for protection of personal data.

This complaint demonstrates the need for data controllers to be aware of their data protection responsibilities, regardless of the situation presented to them. This disclosure of personal data could have been avoided had the veterinary practice simply informed its client that the dog's microchip was no longer registered in his name. There was no justification in this instance for the disclosure of the new owner's name and address details. Data controllers must exercise great caution where they receive requests for personal data of individuals that they are able to access, irrespective of the credibility of the case presented to them by the requester. Having said that we are entirely satisfied that the veterinary practice acted in good faith based on the information provided to it by the dog's previous owner. Equally there was no suggestion during the investigation of the complaint that the dog's previous owner was seeking to act in any untoward manner in relation to the dog's new owner or the dog but rather was simply seeking to arrange contact with his former pet.

Case Study 9: Unlawful use of CCTV to remotely monitor an employee.

In October 2010, I received a complaint from an individual who stated that he considered that his personal privacy was being affected in his workplace through the inappropriate use of a CCTV system which his employer had installed. The complainant was employed by Westwood Swimming Ltd in Leopardstown as an administrator. In support of his complaint the individual cited two separate occasions, three months apart, when he received phone calls from his employer who was not on the premises at the time. In both of these phone calls the employer allegedly described to him what he had been doing at a particular time, i.e. that he was conversing with and working on a computer used by an individual from the office next door (who had a different employer). The complainant stated that subsequent to these incidents he had received two separate written warnings. He also stated that the CCTV system was installed without prior staff notification as to the reason for its installation or its purpose.

My Office contacted Westwood Swimming Ltd and we informed it of its obligations under the Acts in respect of CCTV usage. We advised that any monitoring must be a proportionate response by an employer to the risk he or she faces taking into account the legitimate privacy and other interests of workers. We further advised that in terms of meeting transparency requirements, staff must be informed of the existence of the CCTV surveillance and also of the purposes for which personal data are to be processed by CCTV systems. We provided it with copies of our guidance material on the use of CCTV and staff monitoring. It was asked to outline how the processing of personal data as complained of complied with the Acts and to give details of any signage that was in place on the premises informing individuals that there was CCTV in operation and its purpose.

Westwood Swimming Ltd in response stated that the CCTV system was installed with the priority focus being security of the office due to the amount of cash and credit card slips with customer information on hand. It informed us that a secondary purpose for the CCTV was the fact that it had received numerous complaints from its customers stating that the office was not open or that the office was open and

unattended which gave it further concern for the security of cash/credit cards. It confirmed that its staff had not been informed in writing of the installation and purpose of the CCTV. However, it indicated that staff were well aware of the reasons behind the new system as the cameras were overt and the recorder and screen showing views and recordings were in the office in full view of both staff and clients. It stated that the system was installed during working hours in full view of the staff and no query, question or complaint was received from either the staff or clients. It also referred to having signage in place informing people of CCTV being in operation. In this regard, it provided us with a copy of a notice posted at its main entrance listing the various services available at the centre. While it was noted on the bottom of the signage that CCTV cameras were in operation it gave no indication as to its purpose.

Westwood Swimming Ltd acknowledged that the CCTV footage had been reviewed by it in respect of the incidents cited by the complainant.

After consideration of the response received from Westwood Swimming Ltd, my Office informed it that we were satisfied that it had used a CCTV system to monitor an employee and that such monitoring was in breach of the Data Protection Acts. We asked that it immediately confirm to us that it would cease the practice of monitoring employees by remotely accessing the system from a live feed or by any other means. In response, it provided us with a commitment that its employees would not be monitored remotely or by other means using CCTV. It confirmed that the cameras in the office would be removed, any disciplinary actions taken against the employee concerned on foot of the use of CCTV would be discarded, and that it would ensure that the employee would not suffer as a result of any information seen on camera.

At the request of the complainant, I issued a formal decision on this matter in March 2011 which stated that the leisure centre contravened Section 2(1)(c)(ii) of the Data Protection Acts by the further processing of CCTV images which were stated to have been obtained for security purposes in a manner incompatible with that purpose. These contraventions occurred in the two instances when the CCTV was used to monitor the performance of the complainant in the course of his employment.

The improper use of CCTV to monitor employees is a matter of increasing concern to me. Even where employers have sought to legitimise the use of CCTV to monitor staff by referring to it in their company handbook, the position remains that transparency and proportionality are the key points to be considered by any data controller before using CCTV in this manner. We would only expect CCTV footage to be reviewed to examine the actions of individual staff members in exceptional circumstances of a serious nature where the employer could legitimately invoke the provisions of Section 2A (1) (d) of the Acts ("the processing is necessary for the purposes of the legitimate interests pursued by the data controller …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."). This was clearly not the case in the circumstances which formed the basis of this complaint.

Case Study 10: Financial institutions deny right of access to credit assessments.

I received a number of complaints in the recent past concerning the failure of some financial institutions to comply in full with access requests that are submitted to them by their customers or former customers. A recurring theme with these complaints is the withholding, under the provision set out in Section 4(4A)(b)(ii) of the Data Protection Acts, of personal data contained in credit assessments or submissions to credit committees. This provision allows a data controller to withhold personal data relating to the requester if the data consists of an expression of opinion about the requester where such an opinion was given in confidence or on the basis that it would be treated as confidential.

The exemption to the right of access in this provision is limited to expressions of opinion about the data subject given in confidence which may be contained within a document(s). The exemption does not apply to the remainder of the personal data in the document(s) which is not an expression of opinion about the data subject. It may be the case, for example, that a part, section or sentence within a document is, on its own merit, an expression of opinion given in confidence about a data subject. However, it is highly unlikely that a document would constitute in its entirety an expression of opinion given in confidence about an individual. In most circumstances, a document which contains an expression of opinion would also contain factual information about the individual who is the subject matter of the expression of opinion. I consider that an expression of opinion must be considered in its narrowest sense, namely the view(s) held by a person or entity of a living individual or what one thinks about a living individual. Clearly it does not apply to matter of fact about a living individual.

It follows, therefore, that a data controller may not be permitted to apply a blanket exemption to the right of access over an entire document(s) simply because there are parts, sections or sentences within it which may be considered to be an expression of opinion about a living individual given in confidence. The exemption, where validly claimed, may only be applied to cover the specific elements of the document(s) that constitute an expression of opinion about the data subject given in confidence. A data

controller can comply with the access request and, at the same time, easily give effect to a valid exemption by blackening out the specific expression of opinion and then release the remainder of the document(s).

Some financial institutions have attempted to rely on Section 4(4A)(b)(ii) to restrict access to certain information contained in credit assessments or submissions to credit committees in the consideration of loan applications. However, I consider that an employee who submits in written form their views or opinions on the financial status of a customer does so as part of the day-to-day performance of their own functions as an employee. For that reason, I do not consider that they can validly claim that their views or opinions on the customer concerned enjoy an expectation of confidentiality. A financial services employee must be able to stand over their views or opinions on a customer without trying to conceal their thinking behind the cloak of an expectation of confidentiality.

In cases which we investigated, we upheld the rights of the requesters to access this information and the financial institutions concerned have released the personal data concerned on pain of enforcement. I am putting all financial institutions on notice that any further reliance on this exemption to withhold such personal data will be met with by enforcement proceedings.

Case study 11: Access request for old records.

We received a complaint from an individual concerning the alleged failure of the Public Appointments Service (PAS) to comply with an access request he submitted in March 2010. The personal data which the complainant was seeking access to related to his candidature in recruitment campaigns carried out by the PAS (formerly the Office of the Civil Service and Local Appointments Commission) in the 1960s and 1970s.

In response to our investigation, the PAS confirmed that it was still in possession of the files relating to the recruitment campaigns in question, campaigns that took place over the course of a decade from 1969 to 1979. It also confirmed that it was in the process of identifying all of the personal data relating to the complainant, but it was not a straightforward process given the age of the files, and the fact that some older files had been amalgamated.

The PAS subsequently provided the complainant with copies of the personal data that it had located, but it informed him that it was applying the exemption set out at Section 4(4A)(b)(ii) to other data. This exemption allows for the withholding of data that constitutes an expression of opinion, in circumstances where the expression of opinion referred to was given in confidence or on the understanding that it could be treated as confidential. The PAS argued that the data was created in the 1970s in a culture of confidentiality, long before the introduction of Data Protection or Freedom of Information legislation. Having examined the data it was satisfied that it would not have been created in the first instance but for the understanding that it would be treated in confidence. The PAS indicated that it had an obligation to honour the guarantee given to the individuals concerned in this case and that it would not be prepared to renege on that commitment, even at this stage.

We requested sight of the documents in question to determine whether the exemption at Section 4(4A)(b)(ii) was validly applied. Following an examination, we informed the PAS that some elements of the documents could be withheld, but the exemption could not be applied to the entirety of the documents in question. The PAS followed our advice and released the personal data on that basis to the requester.

We took this opportunity, given the complaint and the issues highlighted by it, to advise the PAS to re-examine its policies in relation to the retention of personal data for longer than was necessary for the purpose/s for which it was obtained. The PAS informed us that it had a Records Retention Policy in place, in accordance with data protection requirements, which sets out the timeframes for the retention and destruction of records. Records such as those that had been examined by my Office on foot of this complaint have a retention period of three years after the determining of the candidate as suitable, or otherwise, for appointment, but in this instance records had been retained by the PAS for over 30 years. PAS indicated that it had applied for, and had only recently received Certificates of Destruction from the National Archives in relation to these records.

As this case shows, data controllers not only need to have a retention policy in relation to the keeping of personal data, but they must also have an effective mechanism in place to implement that policy. Once an access request is received by a data controller, they must provide the requester with all personal data sought, irrespective of the age of the records, once the data is still in existence. The safe destruction of older records in accordance with a data retention policy is a vital aspect of good data protection practice in any organisation and is a critical tool in ensuring compliance with the law.

Case study 12: Access requests to solicitors for copies of files.

My Office received a number of complaints in relation to the failure of solicitors to comply with access requests from former clients. Often the reason cited by the solicitor for not complying with the access request is that they have a common law lien on all documents and papers that constitute work carried out on the client's behalf for which payment remains outstanding.

This issue, where a common law lien on a client's file is considered to apply, is one that we have dealt with and we are not in any way unsympathetic to the scenario for the solicitor in question where a former client is seeking not to pay outstanding fees which are the subject of a dispute. Equally, in the context of a file handled by a solicitor's practice, it is undoubtedly the case that there is far more information on a file than what could be considered to be the requester's personal data and no requirement to provide any information which is not strictly the personal data of the requester arises. However, the Data Protection Acts, which transpose the EU Directive on Data Protection, do not provide any exemption to the provision of the personal data of a person in these circumstances.

A solicitor who has been engaged by an individual is a data controller of that individual's personal data which is subsequently processed. Personal information held by a data controller falls to be released in response to an access request unless a valid exemption as provided for under Sections 4 and 5 of the Data Protection Acts can be relied upon.

The complaints were resolved to the satisfaction of the complainants and the solicitors concerned on the basis of the following guidance from my Office:

- The exemption provided for under Section 5(1)(g) of the Data Protection Acts, which relates to personal data "in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers" applies to personal information held in respect of a solicitor's

capacity as legal adviser to its clients (not the requester) rather than information held in their capacity, or former capacity, as legal representative for the requester.

- In relation to letters from the solicitor acting for another client, it is possible that the restriction to the right of access in Section 5(1)(g) of the Data Protection Acts may apply to any personal data of the requester contained within them.

- Regarding letters generated by a solicitor on behalf of the requester who was a client, a large number of which may have already been sent to them in the normal course of events, i.e. when generated, its difficult to see how a claim of privilege under Section 5(1)(g) would apply where the letters have previously been sent to the requester.

- It is difficult to anticipate that Section 5(1)(g) would apply to attendance notes created by the solicitor in relation to their client. Where notes relate specifically to the client and were created in that context, we would deem the personal data contained in those notes to be valid for release.

Case Study 13: Access to reports compiled by private investigators.

My Office received a complaint from an individual concerning the alleged failure of HSG Zander Ireland Limited to comply with an access request submitted to it in October 2010. The requester was a former employee of HSG Zander Ireland Limited and he informed us that the company had hired a private investigator to monitor him for a period of time. He was particularly eager to access any personal data contained in documentation relating to the surveillance carried out by the private investigator.

We commenced an investigation with HSG Zander Ireland Limited in relation to an alleged failure to comply with the access request. It subsequently provided the requester with a copy of his personnel file but stated that it was withholding the security report compiled by the private investigator by virtue of the exemption under Section 5(1)(g) of the Data Protection Acts 1988 and 2003. This Section restricts the right of access to personal data "in respect of which a claim of privilege could be maintained in proceedings in a court in relation to communications between a client and his professional legal advisers or between those advisers".

It was not obvious to our investigation that a security report compiled by a private investigator could constitute a communication between a client and their professional legal advisers to which a claim of privilege could be maintained in proceedings in a court. On that basis we sought an explanation from HSG Zander Ireland Limited as to its application of that provision to restrict the right of access to the data subject. In response, the company immediately released a copy of the security report and associated photographs to the data subject while maintaining its position that it was entitled to restrict the right of access in accordance with Section 5(1)(g).

We also established in the course of our investigation that there was no contract in place between HSG Zander Ireland Limited and the private investigator who prepared the security report. Engaging the services of a private investigator is no different to engaging the services of any other third party service provider. For that reason, it is unlawful for an entity to pass any details of its employees to a private investigator for the purposes of surveillance or for any other purpose unless that entity has put a

contract in place with in line with Section 2C(3) of the Data Protection Acts 1988 and 2003 which would render the private investigator to be a data processor.

With greater frequency complaints such as this one are coming to my Office regarding difficulties which data subjects are experiencing in accessing security or surveillance reports which have been conducted on them by private investigators. I consider it necessary, therefore, to set down my position in relation to the requisitioning of such reports in the first instance and then the right of access by data subjects to them.

The decision by a data controller to engage the services of a private investigator to gather personal data surreptitiously about a data subject carries very serious risk of breaching the provisions of the Data Protection Acts and the general right to privacy protected by Bunreacht na hÉireann (the Irish Constitution), the European Charter of Fundamental Rights and the European Convention on Human Rights. It should therefore not be taken lightly. Data controllers who hire a private investigator to undertake surveillance on an individual and/or to seek a background or other report from a private investigator on an individual must be aware of and should ensure that the following rules are observed both by themselves and by the private investigator:

I. Prior to passing any instructions to a private investigator in respect of any individual, the data controller should have a written contract in place with the private investigator which meets the requirements of Section 2C(3) of the Data Protection Acts.

II. Any processing of information by private investigators on their behalf must be undertaken in full compliance with the Data Protection Acts.

III. The private investigator is expected to comply at all times with the Data Protection Acts and should not perform their functions in such a way as to cause the data controller to breach any of its obligations under the Data Protection Acts.

IV. Any unauthorised processing, use or disclosure of personal data by the private investigator is strictly prohibited.

V. Where the private investigator, pursuant to its obligations under contract from the data controller, processes the personal data of an individual on behalf of the data controller, the private investigator should:

- Process the personal data only in accordance with the specific instructions of the data controller;
- Process the personal data only as is necessary for the fulfilment of its duties and obligations under the contract with the instructing data controller;
- Implement appropriate measures to protect against accidental loss, destruction, damage, alteration, disclosure or unlawful access to the personal data in their possession;
- At the conclusion of each investigation deliver all data collected and processed under the contract of service to the instructing data controller and delete all such personal data held by itself at that time;
- Not further disclose the personal data to any other party except with the express approval of the data controller;
- Not seek to access personal data held by other data controllers which is not in the public domain without the consent of the data subject or unless otherwise permitted by law.

With regard to the right of access to reports compiled by private investigators, the responsibility to comply with a data subject access request lies with the data controller who hired the private investigator. Where a private investigator receives an access request from an individual, they should transmit that request without delay for processing to the data controller who commissioned them in respect of the particular task. I do not consider that any of the restrictions to the right of access to personal data which are set down in Section 5 of the Data Protection Acts could reasonably be applied to an access request by an individual for a copy of a surveillance report or accompanying photographs or video footage taken by a private investigator. As in the aforementioned complaint, Section 5(1)(g) is invalidly relied on from time to time as a means of restricting access by data subjects to private investigator reports by data controllers or by solicitors who hired private investigators on their behalf. This Section does not equate to privilege at common law (i.e. legal advice privilege and litigation privilege). Instead, this very narrow statutory restriction to the right of access only applies where (i) there is a communication between a client and his professional legal advisors or a communication as between a client's professional legal advisors; and (ii) that is a communication in respect of which a claim of privilege could be maintained in proceedings in a court. A private investigator's report, commissioned by a data controller or by a solicitor acting on behalf of a data controller, is clearly not a communication between a client and his professional legal advisors. Nor is it a communication as between a client's professional legal advisors. For those reasons, the statutory exception in Section 5(1)(g) does not apply to such a report.

I will continue to defend the rights of data subjects to access a copy of private investigator reports and I do not contemplate that any of the limited restrictions to the right of access in the provisions of Section 5 can, as a generality, be validly claimed in such cases.

Appendices

Appendix 1 – Presentations

Appendix 2 – Registration statistics

Appendix 3 – Account of income and expenditure

Appendix 1 – Presentations and Talks

During 2011 my staff and I gave presentations to the following organisations:

Educational

NUI Maynooth – Law Department
University College Galway – Genetic Discrimination Conference
Royal College of Surgeons – MSc in Neurology and Gerontology for physiotherapists Course
Third Level Institutions Admissions Officers Association

Commercial

Society of the Irish Motor Industry – AGM
Wicklow County Enterprise Board – Technology Seminar

Financial Services

Chartered Accountants Ireland – Data Protection in the Cloud Seminar
CUDA - Credit Union Development Association Seminar
Irish Brokers Association X 5 – Data Protection What it Means for Brokers
CUMA – Credit Union Managers Association Annual Conference
Bank of Ireland Regulatory – Risk & Compliance Officers
Credit Union Chapter, Cork – Data Protection Policies & Procedures
Chartered Institute of Internal Auditors – Conference

Health Sector

Voluntary Health Insurance – Continuous Professional Development Session
Trinity College – Lecture to MSc In Health Information Students
Data Protection in Clinical Research – Post Grad Cert in Nursing (Clinical Research)
State Claims Agency – Clinical Indemnity Scheme Seminar
Royal College of Physicians in Ireland – Ethics I: Professionalism course
Health Informatics Association – Annual Conference 2011

Insurance Sector

Insurance Institute of Ireland – Lecture: Data Protection, the thorn in everyone's side

Life Insurance Association Ireland – Seminar Data Protection

International

ENISA – Workshop on Data Breach Notifications

International Association of Privacy Professionals Washington – Tips for dealing with National Privacy Commissioners

International Association of Privacy Professionals European Conference Paris

Data Protection Intensive – Data transfer and data breach conference

Croatian Data Protection Agency – Twinning Project

Legal

Free Legal Advice Centres (FLAC) – General Data Protection Presentation

Mixed Seminars

Information & Records Management Society – Meeting re "Challenges & Opportunities"

Irish Computer Society – Annual Conference 2011

PCI DSS Seminar - Breakfast Briefing

IAPP – KnowledgeNet

Neopost/IDMA – Data Protection Seminar

Association of Compliance Officers (ACOI) – Seminar & Booklet launch

Ireland France Chamber of Commerce – On Premise & Cloud Data Protection Seminar

Irish Computer Society – Direct marketing & eRegulations

Irish Times Training – Breakfast event re the use of cookies

Data Security Seminar – Data Protection & Credit Unions

PDP Conference

Government/Agency

Institute of Public Administration Certificate in Civil Services & State Agency Studies
Public Affairs Irelandx2 Cloud Computing & Ireland + Data Protection Course
Revenue Commissioners – Training seminar
Citizens Information Board – Information Providers Programme
Government Internal Auditors Conference – Heads of Internal Audit Meeting

Political

Oireachtas Briefing on new ePrivacy Regulations implications for members

Religious

Congregation of Sisters of Mary – Data Protection Information Day

Direct Marketing

Irish Direct Marketing Association – Direct Marketing

Telecommunications

Irish Internet Association – briefing on new ePrivacy Regulations
Bandwidth Telecommunications Ltd – General Data Protection presentation.

Appendix 2 - REGISTRATIONS 2011

The total number of register entries in 2011 was 4,940. This figure can be broken down into the following categories:

(a) Financial and Credit Institutions

528

(b) Insurance Organisations

389

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

66

(d) Telecommunications/Internet access providers

39

(e) Health Sector

1425

(f) Pharmacists

950

(g) Miscellaneous

606

(h) Data Processors

811

(I) Government Departments &Offices

126

Total number of registration entries:

2009	2010	2011
4138	4954	4940

In 2011 the number of organisations registered decreased by 14 approximately 0.03%. This decrease reflects the closure of a number of organisations due to the current economic climate.

Appendix 3 - Abstract of Receipts and Payments in the year ended 31 December 2011*

Account of Receipts and Payments in the year ended 31 December 2011

	2011		2010
Receipts	**€**		**€**
Moneys provided by the Oireachtas	**1,523,462**		**1,449,430**
Fees	**587,590**		**590,025**
Other Receipts	**887**		**39643**
Totals	**2,111,939**		**2,079,098**
Payments			
Staff Costs		**1,220,695**	**1,282,087**
Establishment Costs		**144,472**	**151,060**
Legal and Professional Fees		**144,349**	**670**
Incidental and Miscellaneous		**13,946**	**15,613**
		1,523,462	**1,449,430**
Payment of receipts for the year to the Vote for the Office of the Minister for Justice & Equality		**588,477**	**629,668**
		2,111,939	**2,079,098**

**The financial statements of the Office are subject to audit by the Comptroller and Auditor General and after audit are presented to the Minister for Justice, Equality and Law Reform for presentation to the Oireachtas*