

# eDeposit Ireland

## Twenty-First Annual Report of the Data Protection Commissioner 2009

Item Type	report
Authors	Hawkes, Billy
Citation	Billy Hawkes, 'Twenty-First Annual Report of the Data Protection Commissioner 2009', [report], Data Protection Commissioner, 2010-03, Annual reports (Data Protection Commissioner), 21st, 2009
Publisher	Data Protection Commissioner
Rights	Y
Download date	2026-03-14 20:31:50
Link to Item	<a href="https://hdl.handle.net/20.500.14765/81623">https://hdl.handle.net/20.500.14765/81623</a>

**Twenty-First Annual Report of the Data Protection  
Commissioner 2009**

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

**PRN. A10/0163**

# Contents

Part 1 .....	4
Foreword.....	4
Introduction.....	6
Customer Service .....	7
Governance .....	8
Complaints and Investigations.....	8
Use of Legal Powers .....	12
Data Breach Notifications.....	13
Bord Gáis Éireann.....	16
Health Service Executive (HSE).....	16
Privacy audits.....	17
Audit Guidance .....	18
Revenue Commissioners.....	18
Organisations audited in 2009: .....	19
List of Organisations audited.....	20
Motor Tax Circular .....	21
Promoting awareness .....	22
Age-related Awareness Raising.....	23
Video Clip Competition.....	24
Training opportunities.....	24
Policy issues.....	25
Direct Marketing Exemption .....	25
Codes of Practice .....	26
Anti-money laundering .....	28
DNA Bill.....	29
Spent Convictions Bill .....	29
NRA/eFlow .....	30
Health Information Bill.....	31
Health Audit Networks .....	32
Engagement with Ethics Committees .....	33
Communications (Retention of Data) Bill 2009 .....	33
ePrivacy Directive.....	33
Google Street View.....	34
International Responsibilities.....	34
Article 29 Working Party.....	34
International Data Transfers .....	35
Towards new Data Protection Standards? .....	35
Personal Data Accountability .....	36

Third Pillar Groups .....	36
Administration .....	38
Running Costs .....	38
Part 2 .....	39
Case Studies .....	39
Part 3 .....	71
Guidance .....	71
Breach Notification Guidance: .....	71
Direct Marketing - A General Guide for Data Controllers: .....	71
Appendices .....	73
Appendix 1 – Presentations and Talks .....	73
Appendix 2 - REGISTRATIONS 2009 .....	75
Appendix 3 - Abstract* of Receipts and Payments in the year ended 31 December 2009.....	76

## List of tables and figures

Table 1 - Enforcement Notices .....	13
Table 2 - Information Notices.....	13
Table 3 - Running costs .....	38
Figure 1 - Complaints opened, concluded and outstanding.....	9
Figure 2 - Breakdown of complaints by issue .....	11
Figure 3 - Number of complaints received since 2000 .....	11
Figure 4 - Organisations reporting breaches by sector .....	15
Figure 5 - Type of data breach.....	15

# Part 1

## ***Foreword***

2009 was a year of change - both actual and promised - in the legal framework governing data protection.

The Lisbon Treaty embedded data protection as a fundamental right of European Union citizens. It provided the basis for an extension of data protection rights into all areas of EU activity. It gave new authority to the European Parliament as co-legislator in this area.

There was increased recognition of the international dimension of data protection. An outline of an international standard on data protection was approved by the International Conference of Data Protection and Privacy Commissioners. There was significant progress in work being done to the same end within the International Standards Organisation and in the APEC (Asia-Pacific) region. Developments within the European Union further facilitated the safe transfer of personal data to other regions of the world. The interest of international business in these developments was demonstrated by their active involvement in an *Accountability* project facilitated by our Office.

In Ireland, increasing government concern at data breaches led to the establishment of a working group to examine the possible need for legislative change in this area. Such change would reflect the new provisions introduced at EU level in the revised *ePrivacy* Directive. We have been actively involved in promoting best practice in this area through our guidance and audit activities.

Data protection principles have stood the test of time. The challenge of giving practical effect to the fundamental right to protection of personal data remains.

Rapidly changing technology can be both a threat to this right and the means of protecting it. Building data protection safeguards into new technologies and applications of these technologies remains the best approach. This is as much true of data processing in the "cloud" as it is of a routine development of an IT application in an organisation.

During the year, we continued to use the full "tool-kit" provided to us by law to advance the data protection rights of individuals. Most organisations do their best to respect the rights of their customers and clients - recognising that this is also an issue of good customer service. For them, our focus continued to be on advice on how best to meet their obligations. For the minority who are careless about data protection rights, we used the full range of our enforcement powers to bring about change. Targeted use of prosecutions has been particularly effective to stamp out abuses in the area of electronic marketing. Selective use of our audit and investigation powers have also helped to bring about improvements at sectoral level.

An area of some disappointment has been the reluctance of some State bodies to take sufficient account of data protection issues when framing new legislation or applying existing law. In some such cases, I have, reluctantly, felt it necessary to bring concerns directly to the attention of the legislature. In all such cases, I try to fully recognise the difficult balancing act that is often required to take account of issues such as security, fraud and administrative efficiency.

As I come to the end of my 5-year term of office, I wish to pay a warm tribute to the staff of the Office. Despite reduced resources, they have continued to work cheerfully and patiently to make data protection a reality for all who come in contact with us.

*Billy Hawkes*

*Data Protection Commissioner*

*Portarlington, March 2010*

## ***Introduction***

The Lisbon Treaty, which entered into force in December 2009, embedded data protection as a Treaty-guaranteed fundamental right in the European Union's legal order. A framework decision on data protection in EU police and judicial cooperation entered into force in January. A revised e-privacy directive approved in November will strengthen the powers of national data protection authorities to address breaches of privacy in the telecommunications area. In this country, the Minister for Justice, Equality and Law Reform established a Data Protection Review Group to make recommendations on whether Irish data protection legislation needs to be amended to provide for mandatory notification of data security breaches and for the imposition of penalties where necessary. With all these developments, it would be comforting, but misleading, to imagine that our data protection rights are well-entrenched and our privacy is therefore adequately safeguarded.

Despite efforts to raise awareness of data security issues, data security breach reports from both private and public sector organisations increased in 2009. While the performance of some organisations has undoubtedly improved, I remain disappointed with the continuing security problems within particular sectors. It was also disappointing that my Office felt obliged to prosecute several organisations, mostly in relation to unsolicited electronic communications.

Proportionate and well thought out security measures can be a valid response to concerns about terrorist or other threats. Similarly, fair and legitimate commercial processing of personal data is perfectly acceptable. Understandably, those who are responsible for the security of our state want our security infrastructure to be as strong as possible. In a difficult commercial environment, private companies are driven to seek every possible advantage. Problems arise when security or commercial interests are allowed to take unquestioned precedence over the privacy rights of the individual. The State must protect individual human rights (including the right to privacy) or risk oppressing its citizens and ultimately strengthening its enemies. Commercial companies that ignore individual privacy rights risk handing an advantage to competitors (and a potential prosecution). My Office will continue to promote

proportionate, fair and balanced practices on the part of public and private sector bodies - in everybody's interests.

### ***Customer Service***

As a public office, I consider that customer service is of great importance and we retain a focus on the provision of comprehensive and practical information and advice on data protection to all our customers. Indeed much of the day-to-day work of the Office entails the provision of advice and information in response to enquiries received either in person, by phone, by email or by post. Our website, [www.dataprotection.ie](http://www.dataprotection.ie), remains our key point of contact with our customers. Content is regularly reviewed to ensure that it is accessible, up-to-date and accurate. As part of this broad effort we are currently developing a new layout to increase the accessibility of this key customer tool. We try to ensure that all the tasks that we undertake - audits, investigations and enforcement - contribute to our broader goal of ensuring that members of the public are aware of and demand their rights and that organisations are aware of their corresponding obligations. During 2009 we continued our practice of involving the entire team in the provision of advice and information directly to our customers so that everyone is in touch with their concerns.

Our interaction with the media continues to be a valuable means of raising awareness of data protection issues. We try to make staff available to respond to queries and requests for interviews to the maximum extent possible, allowing us to communicate best practice in response to emerging data protection issues. Last year my Office dealt with over one hundred queries from the media.

We also try to maximise our accessibility to business, NGOs and public sector organisations. Members of the ODPC team make public presentations on data protection as part of their duties in so far as we possibly can. These presentations are given in response to invitations from groups in the private or public sector that want an opportunity to learn more about their data protection rights and responsibilities. We have found that these events provide an excellent opportunity to discuss privacy issues in the context of new technologies, products and challenges. Details of our presentations in 2009 are given in Appendix 1 – Presentations and Talks of this report. While we try to accept such invitations to the maximum extent possible,

unfortunately resource constraints on the Office necessitate that they cannot all be accepted.

I encourage a 'train the trainer' approach through the provision of guidance material and learning aids on my Office's website where it is not possible for my Office to give a presentation.

Our Irish Language Scheme under the Official Languages Act 2003 has been in effect for four years. During that time my Office has made great progress in providing services to customers in both Irish and English and in ensuring that key information is available on our Irish language website, [www.cosantasonrai.ie](http://www.cosantasonrai.ie). In the early months of 2010 we developed a new Irish Language Scheme aimed at copper fastening the progress already achieved.

### ***Governance***

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

My Office utilises core systems and services provided by the Department of Justice, Equality & Law Reform - 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.

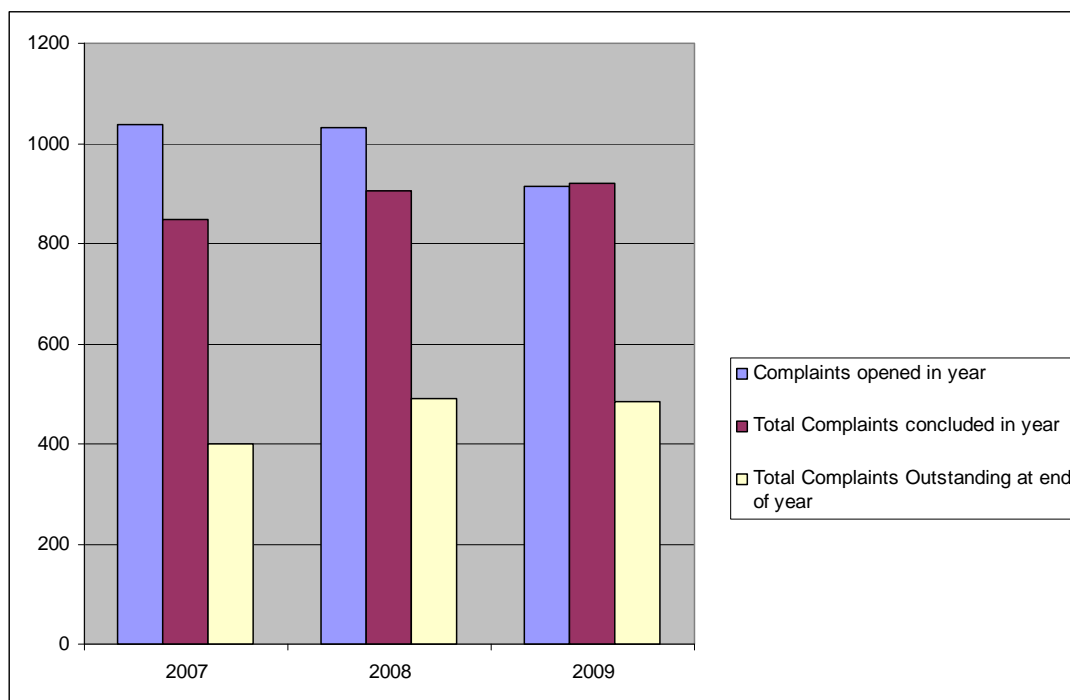
### ***Complaints and Investigations***

My Office continues to receive significant numbers of complaints from members of the public in relation to the treatment of their personal data. In 2009 a total of 914 complaints were formally opened for investigation by my Office, representing a slight reduction in the numbers opened in recent years (1,031 complaints were opened in 2008 and 1,037 complaints in 2007). It is likely that this slight decrease can be accounted for by the increased focus in my Office on identifying the relevant data protection issues in complaints at first instance and seeking to resolve such matters

informally where possible or to seek additional information from a complainant to support a complaint. The continued high volume of complaints places a considerable burden on my Office's Investigation Unit and on the resources of my Office generally.

Figure 1 - Complaints opened, concluded and outstanding - illustrates the numbers of complaints opened, concluded and outstanding in 2007, 2008 and 2009.

**Figure 1 - Complaints opened, concluded and outstanding**



I am very pleased to report that the 2008 trend of a significant decrease in the number of complaints which fall under the Privacy in Electronic Communications Regulations (S.I. 535 of 2003 as amended) has continued. In 2009 we opened a total of 262 complaints in this category reporting unsolicited direct marketing text messages, phone calls, fax messages and emails. This compares with 321 such complaints in 2008 and 538 in 2007. In the last two years, therefore, complaints in this area have halved. As we reported last year, a number of factors have combined to bring about a welcome decrease in this category of complaint (which in many cases constitute criminal offences). There is greater awareness among marketing companies of legal

requirements governing the use of phone numbers which are entered on the National Directory Database Opt-Out Register. As the number of phone numbers entered on that Register continues to grow, complaints concerning cold calling continue to decrease. Regarding unsolicited marketing text messages, my Office opened 50 fewer complaints in 2009 than in 2008, and almost 250 fewer complaints than in 2007. This decrease can be attributed to the effect on the text marketing sector of prosecution proceedings which I lodged in the District Court towards the end of 2007 against a number of companies operating in the premium rate text messaging sector. Many of those cases were eventually heard by the District Court in 2009. I successfully prosecuted four companies operating in the premium rate text messaging sector in 2009 for offences under S.I. 535 of 2003, namely Opera Telecom (Ireland) Ltd, Zamano Solutions Limited, Mountwilson Ltd and Púca Technologies Ltd (in its capacity as a provider of the SMS technology and network used for the sending of messages by a client). A number of other summonses lodged in the District Court in 2007 have yet to be heard and I expect that these will be successfully concluded later this year.

In addition, outside of the premium rate text messaging sector, I also prosecuted Map Dance Ltd (trading as Jackie Skelly's Gyms) and Home RBVR Ltd (trading as Brasserie 66 restaurant) in 2009 for offences relating to the sending of unsolicited marketing text messages. Separately, I prosecuted Prism Fax Services Ltd in 2009 for the sending of unsolicited marketing fax messages. I will continue to exercise my powers of prosecution in 2010 for offences under S.I. 535 of 2003 (as amended). The message from my Office is clear - entities that continue to commit offences in relation to electronic marketing face prosecution and where my investigations establish that offences have been committed I will use my powers of prosecution against those entities who commit them and do not learn from their mistakes.

	<b>2009</b>
Access Rights	29%
Electronic Direct Marketing	28%
Disclosure	17%
Unfair obtaining of data	5%
Failure to secure data	4%
Unfair processing of data	3%
Accuracy	2%
Use of CCTV footage	2%
Excessive data requested	2%
Postal Direct Marketing	2%
Unfair retention of data	2%
Other	4%

**Figure 2 - Breakdown of complaints by issue**

Figure 2 - Breakdown of complaints by issue illustrates the breakdown of complaints by data protection issue. After a big increase in 2008, complaints in relation to breaches of the Data Protection Acts, 1988 & 2003 have decreased slightly from 710 in 2008 (which was 69% of the overall total) to 652 in 2009 (72% of the overall total). Complaints concerning access rights accounted for 29% of complaints overall. A total of 259 such complaints were opened in 2009 compared with 312 complaints about access rights in 2008 and 187 in 2007. This reflects a greater level of public awareness of the right of access to personal data, a key fundamental right enshrined in data protection legislation.

Year	Complaints Opened
2000	131
2001	233
2002	189
2003	258
2004	385
2005	300
2006	658
2007	1037
2008	1031
2009	914

**Figure 3 - Number of complaints Opened since 2000**

When a complaint is opened under the Data Protection Acts, I am required by Section 10 of the Acts to investigate it and to try, in the first instance, to arrange an amicable resolution. I do not open investigations where there is no prima facie basis to form a view that the Data Protection Acts were breached based on the information provided to me. I can also deem that a complaint is ‘frivolous or vexatious’ and therefore no requirement to investigate arises (it is very rare for my Office to have to consider that a complaint falls into that category). As in previous years, the vast majority of complaints concluded in 2009 were resolved amicably without the need for a formal decision under Section 10 of the Acts. In 2009 I made a total of twenty-four formal decisions. Two of these rejected the substance of the data subject’s complaint, two partially upheld the complaint and the remaining twenty fully upheld the complaint. This was a substantial increase on the number of formal decisions I issued in 2007 (ten) and 2008 (seventeen).

As Commissioner, I do not have the power to award compensation. However, if a data controller fails to observe their duty of care in respect of personal data, they are liable to be pursued for damages through the courts (under Section 7 of the Acts). My Office has no function in relation to any such proceedings (which I understand are rarely instigated).

### **Use of Legal Powers**

In my Annual Report for 2007, for the first time, I included a list of occasions when I have had to resort to the use of my legal powers to advance an investigation. This involves serving Enforcement Notices or Information Notices as provided for in the Acts. Details of selected Enforcement Notices and Information Notices served by me in 2009 are set out in the following tables. I hope that publication of these lists will encourage all organisations that are the subject of complaints to co-operate fully with my Office in relation to our statutory investigations. I have not included Enforcement Notices where the organisation has exercised its right of appeal to the Circuit Court. 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 engage with my Office without the need for a formal legal notice to advance an investigation.

**Table 1 - Enforcement Notices**

<b>Data Controller:</b>	<b>In relation to:</b>
Iarnród Éireann	Section 4 (1) of the Data Protection Acts
Iarnród Éireann	Section 4 (1) of the Data Protection Acts
Banta Global Turnkey Limited	Section 4 (1) of the Data Protection Acts
Ice Broadband / Ice Communications Ltd.	Section 3 of the Data Protection Acts

Table 1 - Enforcement Notices<sup>1</sup> issued in 2009

**Table 2 - Information Notices**

<b>Data Controller:</b>
Dunnes Stores
Ice Broadband

Table 2 - Selected Information Notices<sup>2</sup> issued in 2009

### ***Data Breach Notifications***

During 2009, my Office received 119 data security breach notifications. This is a significant increase on the 81 breach notifications received in the preceding 12 months.

Rather than an increase in the absolute number of data security breaches, I attribute this increase to a greater awareness among organisations of their data protection responsibilities. As a matter of good practice when faced with a data security breach, more organisations are contacting my Office for advice on how to deal with the matter. I welcome this development, though obviously I would prefer to see evidence of a reduction in the number of data security breach incidents.

A total of 86 organisations (some organisations reported more than once) notified my Office of data security breaches in 2009. Sixty of these organisations were in the private sector and twenty six organisations were in the public sector. This is an

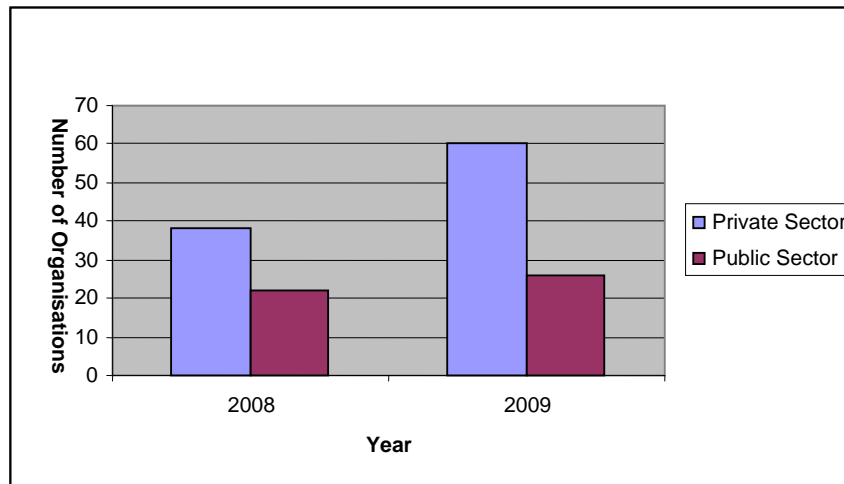
---

<sup>1</sup> 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.

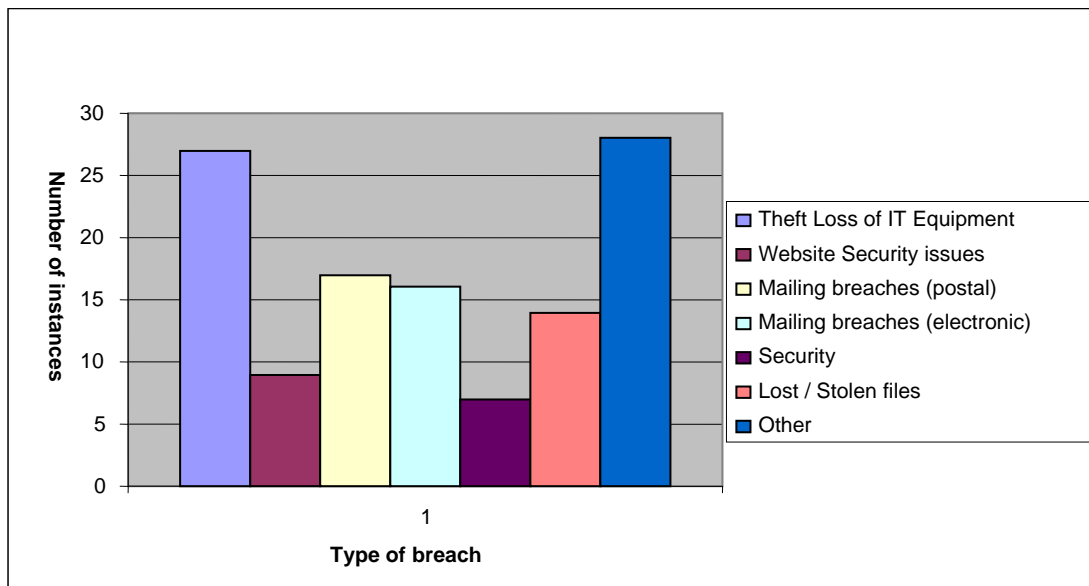
<sup>2</sup> Under section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a person to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation.

increase of 26 organisations reporting breaches to my Office on last year (see Figure 4 - Organisations reporting breaches by sector). The most common cause of reports to my Office is the theft or loss of IT Equipment. We received 27 reports of such incidents (see Figure 5 - type of data breach). This includes the loss or theft of laptops and mobile storage devices such as USB memory sticks. As the use of such devices is now very common and given their capacity to hold large amounts of data, it is very important that organisations ensure that a valid business need exists for personal data to be held on such devices and that appropriate security is in place on the device. At this point there really is no excuse for any organisation placing personal data on a portable device without securing that device properly.

The next biggest cause of data breaches reported to my Office is in relation to mailing, both postal and electronic. There have been 17 reported incidents involving postal breaches. These have involved such issues as incorrect addressing and the inclusion of other individuals' data in an envelope. While it may seem that there would be little impact from this type of incident, several of the incidents reported involved a large batch of letters and many contained financial details that could cause distress or damage to individuals. In relation to the reported incidents of electronic mail breaches (16), many involved disclosing e-mail addresses to other individuals who were also recipients of an e-mail. There is a simple remedy to this problem; organisations must use the Blind Carbon Copy (BCC) field when sending an e-mail to a number of individuals and should have documented procedures in this regard to ensure that all staff are aware of their responsibilities.



**Figure 4 - Organisations reporting breaches by sector**



**Figure 5 - type of data breach**

I welcome the practice of voluntarily reporting data security breaches to my Office (there is currently no specific obligation on organisations to inform either my Office or the individuals affected). As I reported in my Annual Report last year, the Minister for Justice, Equality & Law Reform established a High Level Group on Data Breach Notification to advise him on whether changes to data protection legislation are necessary in this area. The Group published a consultation paper in November and, at time of writing, its final report is expected shortly.

Another security vulnerability that came to our attention during the year was the prescription of readily-known pieces of information - such as date of birth or mother's maiden name - as passwords for access to services. It is essential that organisations, in considering the basis on which they permit access to personal data, ensure that such access is properly safeguarded against abuse by third parties.

Certain security breaches attracted a considerable amount of attention among members of the public concerned at the implications of the cases for their personal privacy.

### **Bord Gáis Éireann**

In June I launched an investigation in relation to a significant loss of personal data arising from the theft of a laptop computer held by Bord Gáis Éireann which had reported the matter to my Office upon becoming aware of the theft. The information included records relating to “Big Switch” customers<sup>3</sup>, including names, addresses, email addresses and financial data. Throughout the process Bord Gáis Éireann co-operated completely with the conduct of the investigation. The investigation concluded that Bord Gáis Éireann failed to have security measures on the stolen laptop that were appropriate to the harm that could result to individuals from the loss of their personal data. As well as an apology to those affected by this incident, Bord Gáis Éireann's efforts to reach an amicable resolution to the complaints which I received included a substantial donation to the Peter McVerry Trust.

### **Health Service Executive (HSE)**

Also in June I launched an investigation in relation to a report from the HSE that a robbery at the HSE West PCCC<sup>4</sup> Offices in Roscommon had resulted in the theft of an unencrypted laptop containing personal data related to clients of the HSE. The HSE cooperated fully with the conduct of the investigation. The investigation concluded that the HSE failed to have security measures on the stolen laptop that were appropriate to the harm that could result to individuals from the loss of the data. I note that the HSE was also mentioned in the context of breach reports in my Annual Report for 2008. Therefore the recommendations of my Office in regard to this incident were extensive and demanding:

---

<sup>3</sup> Customers who had chosen to move electricity supplier from the Electricity Supply Board

<sup>4</sup> Primary, Community and Continuing Care

- The HSE must take organisational responsibility for the encryption of all laptops; it is not sufficient to delegate this responsibility to individual staff members. All HSE areas should make the appropriate arrangements with their laptop suppliers to ensure that laptops are encrypted before they are allocated to staff members. The level of encryption should be regularly reviewed to ensure that it reflects the highest standards currently used in the Irish public service. Steps must be taken to ensure that previously issued laptops are encrypted or to prevent the use of such laptops for any purpose involving personal data.
- The HSE must introduce policies to prevent situations arising in which they do not own or control devices storing HSE patient data.
- The HSE should prioritise the development of secure networks and devices for the transfer of patient data.
- The results of the investigation indicate that the existing controls on patient database development within the HSE are insufficient to prevent the development of ad-hoc databases. HSE staff should be trained to recognise when the creation of a record amounts to a new database and to understand the nature of the controls around such developments.
- The development of appropriate controls governing access to patient databases, including directory services, should be a priority for the HSE.
- Staff training should be further improved to ensure that all staff, particularly at management level, understand the need to report serious data security breaches to the appropriate Consumer Affairs Area Office and, through them, to the ODPC. The HSE should develop a comprehensive breach management policy to cover all forms of data security breach including those involving manual data.

I will be following up progress in this regard.

### ***Privacy audits***

I am empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches.

Scheduled audits are intended to assist a 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 with unscheduled inspections under powers conferred under section 24 of the Data Protection Acts in response to specific issues of concern.

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. Upon conclusion of the audit process, a final report is issued to each organisation audited containing a set of findings and recommendations based on my audit team's examination of key systems processing personal data within the organisation.

Priorities and targets for audit are identified taking account of complaints and enquiries to the Office. During 2009 my Office continued to adopt a proactive role in this regard. In the course of the year, over thirty comprehensive audits were carried out.

### **Audit Guidance**

At the beginning of 2009, I published guidance on audits aimed at assisting organisations selected for audit by the Office of the Data Protection Commissioner - <http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf>. The audit resource also provides organisations holding personal data with a simple and clear basis to conduct a self-assessment of their compliance with their obligations.

### **Revenue Commissioners**

In 2008, I commenced an audit of the Revenue Commissioners, as a public sector entity holding substantial amounts of personal data. The initial stages of the audit programme were focused on obtaining an overview of the organisation in terms of the capture and movement of personal data within it. This initial exploratory stage allowed the audit team to identify priority areas, systems and processes for inspection. The audit took place over a number of dates between November 2008 and May 2009 in various locations across the country.

The audit of Revenue focused on ascertaining and verifying the exact legal basis for each data transfer, the means by which such information is disclosed to Revenue and the channels deployed for any outward bound disclosures. I sought evidence and assurance of the safe and secure transmission of all personal data contained in these transfers. Internal Revenue repositories for the storage and retention of large volumes of personal data were examined in detail in order to assess the efficacy of the policies and procedures in place to safeguard the data held by Revenue.

My Inspection Team found a very high organisational awareness of data protection principles in Revenue and the resulting report commended Revenue for this, at the same time outlining a series of recommendations concerning data retention, privacy impact assessments, data transfers, data protection training and laptop security. I will continue to liaise with the Data Protection Unit in Revenue to ensure that these recommendations are acted upon.

I am pleased that Revenue took the decision to publish the audit report in full on its website:

[Report of the Data Protection Commissioner on Data Protection in Revenue](#)

(<http://www.revenue.ie/en/about/data/data-protection-commissioner-report.pdf>)

### **Organisations audited in 2009:**

In the course of 2009, 30 audits were carried out by my Office. This is an increase on the previous year in which 28 audits were completed. I intend, resources permitting, to continue this level of audit frequency in 2010.

In selecting target organisations for audit, our aim is to reach a broad mix of public, private and voluntary sector entities holding personal data. Audit targets may be selected, for instance, on foot of complaints received by my Office or on foot of specific allegations in media reports etc. However, many organisations are selected for audit purely because they are representative of a particular sector. In most cases it is my hope that the conduct of an audit in a particular sector will have a multiplier effect across a sector and serve to raise standards generally. Such audits also help us

to better understand the challenges faced by organisations and to produce more relevant guidance material.

My inspection teams found that there was a reasonably high level of 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. I note with satisfaction that the majority of the data controllers audited have demonstrated a willingness to put procedures in place to ensure they are meeting their data protection responsibilities in full. I would like to thank all of the organisations audited and inspected throughout the year for their cooperation.

I encourage organisations to agree to the publication of the audits we carry out, as an aid to good practice at sectoral level. I am happy that a number of the audited organisations agreed to such publication.

### **List of Organisations audited**

Joint National Internet Research (JNIR)

Dublin Airport Driving School

Higher Education Authority

Eumom

National Roads Authority (Operation of M50 barrier free tolling)

Eircom

Irish Rugby Football Union

Cedar Clinic

Prescreen.ie

Alzheimer's Society

Central Applications Office (CAO)

Tullamore Credit Union

Vodafone

Primacare Dundrum

Medical Centre Newbridge

Superquinn

Allied Foods  
Mazda  
All Ireland League Rugby Club  
Corduff Community CCTV  
Lidl  
Allianz  
VHI  
Dublin Airport Authority  
St Attracta's School Tubercurry  
AIB Tullamore  
NIB Athlone  
Dundrum Credit Union  
Experian  
Boran Plastic Packaging

### **Motor Tax Circular**

In the last quarter of 2008, my Office conducted an audit of Laois Motor Tax Office and an audit of the National Vehicle & Driver's File (NVDF) at the Driver and Vehicle Computer Services Division (DVCSD), Department of Transport, in Shannon Co. Clare. During that same period my Office attended and presented at a national Motor Tax Conference targeted at authorised officers employed in motor tax offices across the country.

A key issue to emerge from my engagement with this sector was the concern expressed by practitioners themselves regarding procedures around the release of the personal data of drivers to third parties. The attention of my Office was directed to an array of both primary legislation and Statutory Instruments (SIs) providing for the release of certain driver and vehicle data to a range of third parties some of whom were specifically listed. Alongside these there also existed another set of SIs featuring provisions whereby unnamed third parties could request basic driver data.

My Office was made aware that on an increasingly frequent basis, individual Motor Tax Offices were receiving requests for driver data from various insurance and other

similar services. Such requests typically sought to verify not only an individual's licence, but also an individual's licence history, including details of penalty points, disqualifications or convictions. With regard to sensitive data such as penalty points and road offence convictions, the Data Protection Acts were being invoked by way of a type of 'enforced subject access request'; data subjects seeking insurance or renewal of insurance would sign a declaration agreeing to the release of information held on the NVDF to a third party such as an insurance company or an employment screening company. After a review of the sector via the audit findings and direct consultation with both practitioners and policy makers, I reiterated a previously conveyed view of this Office in similar circumstances that a request (signed by the individual and forwarded by a third party) for penalty point data or copies of endorsements on licences held by a Motor Tax Office could not be considered as the 'free' or 'valid' consent of the data subject as would be required to engage the provisions of Section 8(h) of the Data Protection Acts.

I was pleased therefore to note that in 2009 new guidelines were issued by the Department of Transport to all motor tax offices addressing the disclosure of driver data held on the National Vehicle Drivers File (NVDF). My Office was consulted regarding the content of the guidelines.

The guidelines outline the conditions under which it is possible for a third party to make a legitimate request for **basic** driver data on behalf of another individual. However, with regard to sensitive data such as penalty points, the guidelines state that detailed data will only be issued through the post to the data subject or provided to his/her legal representative.

### ***Promoting awareness***

Educating individuals about their rights under the Data Protection Acts and ensuring that organisations are aware of their responsibilities remains a key focus of my Office. The reduced budget available to my Office in 2009 meant that the range of our activities in this area was not as extensive as in previous years.

In 2009, I continued to pursue an awareness campaign targeted at young people and I also extended my targeted activities to include the over 65s. Another awareness-raising initiative, a video clip competition hosted on YouTube entitled '**Private I, Public Eye**', was organised by my Office in 2009 in association with Google.

### **Age-related Awareness Raising**

The findings from the 2008 Public Awareness survey<sup>5</sup> indicated lower levels of awareness amongst the upper and lower age groups (65+ and 15-24 year olds).

In terms of the 12-18 year old cohort, in 2009 I continued to highlight and promote a data protection resource produced by my Office in 2007 aimed at second level schools - '**Sign Up, Log In, Opt Out: Protecting Your Privacy & Controlling Your Data**' ([http://www.dataprotection.ie/docs/CSPE\\_Booklet/862.htm](http://www.dataprotection.ie/docs/CSPE_Booklet/862.htm)). I was pleased to note the inclusion of a question on the CSPE 2009 Junior Cert Examination concerning CCTV (Closed Circuit Television). I am hopeful that there will be further questions on CSPE examination papers reflecting other topics and issues addressed in the '**Sign Up, Log In, Opt Out**' resource. I am also aware of the data protection question which appeared on the Leaving Cert Business Studies Examination Paper (Ordinary Level) in 2008. All of this is indicative of the growing incorporation of privacy-related issues into the Irish educational curriculum.

With regard to the over 65's, I submitted several articles for publication to Ageing Matters - an Age Action Ireland publication. In these articles I highlighted key rights under data protection including access rights, the right to opt-out from marketing and I also drew attention to the need for online security measures. I was pleased to be informed by Age Action that the online security material produced by my Office is being used in free computer classes delivered by Age Action to the over 55s.

---

<sup>5</sup> Survey Key Findings:

<http://www.dataprotection.ie/documents/trainingandawarenes/PAS08.pdf>

Survey Full Report: <http://www.dataprotection.ie/documents/press/Survey08.pdf>

## **Video Clip Competition**

An innovative video clip competition was launched in 2008 by my Office in association with Google. This competition was hosted on my Office's YouTube channel ( [www.youtube.ie/dataprotection](http://www.youtube.ie/dataprotection) ). In 2009, I decided to run the competition again, replacing the 2008 theme of '**Privacy in the 21st Century**' with the theme '**Private I, Public Eye**'. The competition had a total prize fund of €10,000 generously provided by Google and attracted a high standard of entries that provided a creative and entertaining look at a range of privacy issues. In an effort to focus on the 18-24 year old age group, I particularly targeted third level colleges where digital media courses were being taught.

The winning clips are available to view at:

First prize [www.youtube.com/watch?v=a5V8OCJA6jA](http://www.youtube.com/watch?v=a5V8OCJA6jA)

Second prize [www.youtube.com/watch?v=BiQ\\_2h-CwPU](http://www.youtube.com/watch?v=BiQ_2h-CwPU)

Third prize [www.youtube.com/watch?v=EbHzi8RQD8A](http://www.youtube.com/watch?v=EbHzi8RQD8A)

Gallery of entries to the competition <http://www.youtube.ie/dataprotection>

## **Training opportunities**

In response to a number of high profile data breaches and cases concerning inappropriate employee access to personal data held by a public sector data controller, a special training initiative targeted at the Civil Service was held in Dublin in February 2009 jointly organised with the Centre for Management and Organisation Development (CMOD) in the Department of Finance. As well as presentations by staff members from my Office, I was pleased at the participation of the Department of Social & Family Affairs and CMOD in delivering presentations to the large audience present.

I continued to promote awareness of data protection rights through the Citizens Information Centres by provision of advice and participation in the Information Providers Programme and I also engaged with the Money Advice & Budgeting Services on similar lines in 2009.

My Office was invited to participate in the Garda College Human Rights Community Fair in April 2009. This event offered the opportunity to promote awareness amongst Garda students of the data protection considerations involved in everyday policing practice.

In the private sector, I gave a significant number of presentations to the insurance sector throughout 2009. I did this in light of the publication by my Office in 2008 of a Code of Practice for the Insurance Sector and the ensuing need to inform and ensure the sector is in a position to comply with all areas of the Code.

The following training aids and guidance material are available free of charge to assist organisations in raising staff awareness of their responsibilities when processing personal information:

( [http://www.dataprotection.ie/docs/Publications\\_and\\_Forms/960.htm](http://www.dataprotection.ie/docs/Publications_and_Forms/960.htm) )

1. Booklet - A guide for Data Controllers
2. Booklet - A guide to your Rights
3. Training DVD - 'My Data, Your Business' and Facilitator's Guide to DVD
4. PowerPoint Presentations
5. Rights & Responsibilities Chart
6. Sign Up, Log In, Opt Out: Protecting Your Privacy & Controlling Your Data
7. Audit Resource (January 2009)

Hardcopies of the booklets, chart, DVD and Facilitator's Guide can be obtained by contacting my Office.

## ***Policy issues***

### **Direct Marketing Exemption**

In the lead-up to the June Local Government Elections, my Office received a large number of complaints regarding unsolicited text messages, emails or phone calls from candidates for election or political parties. I found it somewhat unsatisfactory to have to inform these complainants that I was unable to launch investigations into these

contacts, even when the complainant had made clear that they did not wish to be contacted. This is because of the definition of direct marketing in the Data Protection Acts:

"'direct marketing' includes direct mailing other than direct mailing carried out in the course of political activities by a political party or its members, or a body established by or under statute or a candidate for election to, or a holder of, elective political office."

The definition excludes any direct marketing carried out for political purposes by political parties or electoral candidates from the scope of the Data Protection Acts. While I have doubts about the consistency of this definition with EU Directives in this area (doubts that I brought to the attention of the Department of Justice, Equality and Law Reform), given the present legislative position I could not investigate these complaints. I would suggest that this is an area that may need to be revisited to ensure that individuals can at least refuse the receipt of such communications going forward if they simply do not wish to receive them.

I also received a number of complaints from individuals who were concerned about the manner in which their details were accessed by the candidates for election to facilitate the contact that was made. Where sufficient evidence was provided I investigated such complaints and, in a number of cases, I found that the contact details of individuals were provided or sourced in contravention of the Data Protection Acts. While the Data Protection Acts provide somewhat generous exemptions to facilitate the conduct of political and electoral activity, I would remind all candidates for election and political parties that it is not appropriate to source the details of individuals from any available source and that doing so may bring them into conflict with the requirements of the Data Protection Acts.

### **Codes of Practice**

As I indicated in last year's report, the Department of Finance established a working group in the latter part of 2007 to examine standards for the protection of personal data in the public sector in Ireland. That working group produced an extensive Guidance Note on Protecting the Confidentiality of Personal Data towards the end of

2008 ([http://www.ict.gov.ie/docs/Data\\_Protection\\_Guidelines.pdf](http://www.ict.gov.ie/docs/Data_Protection_Guidelines.pdf)). At the same time all Government Departments, Offices and Bodies were encouraged to prepare a Code of Practice for their handling of personal data to be approved by my Office. I welcome this development. As of 1 March 2010 I have received two such draft Codes. While it is likely that some public sector organisations are waiting until I have approved the first Code, I consider this response to be somewhat disappointing. I would encourage public sector organisations to approach my Office with their draft Codes as a means of assisting them in improving their personal data handling practices.

### **Automatic Number Plate Recognition**

As part of our ongoing and very constructive engagements with An Garda Síochána during 2009, we finalised discussions in relation to the rollout by An Garda Síochána of an Automated Number Plate Recognition (ANPR) system. The ANPR system involves an in-car camera that reads the Vehicle Registration Numbers (VRNs) of other vehicles on the road and then checks each VRN against a database of watch lists. If a 'hit' is detected then an audible signal is given to the members of An Garda Síochána in the vehicle and a picture of the vehicle, its VRN and other relevant information are displayed on the in-car camera screen allowing the members of An Garda Síochána to take appropriate action, as required. The benefits of the technology in supporting certain functions of An Garda Síochána are clear, however this Office must focus on ensuring that any large-scale recording of personal data is proportionate under the Data Protection Acts and that acceptable safeguards as to the uses and storage of, as well as access to, the information are in place.

The Data Protection Acts contain provisions permitting law enforcement agencies to process personal data for investigation purposes, however the retention of data collected by this system in respect of law abiding citizens also had to be considered and a balance as to its retention reached. In this regard, we agreed an ANPR policy document with An Garda Síochána. The guidance contained in this document aims to ensure that those deploying and operating ANPR can do so effectively while also recognising and respecting the rights and privacy of individuals.

## **Anti-money laundering**

In July 2009, the Minister for Justice, Equality and Law Reform published the Criminal Justice (Money Laundering) Bill 2009 which will transpose the third EU Money Laundering Directive into Irish Law. The third EU Money Laundering Directive increases the obligations on credit and financial institutions and on lawyers, accountants, estate agents and others in relation to money laundering and terrorist financing throughout the European Union. It is of particular relevance from a data protection perspective that the Bill confers additional obligations on designated bodies covered by the legislation to perform certain due diligence operations to identify customers.

Prior to the Bill's publication, my Office made submissions in relation to the draft Heads of the Bill. This provided a very welcome opportunity for us to input views into the drafting process to seek an appropriate balance between the sometimes competing requirements of money laundering legislation and data protection legislation. We know that, in the past, a large number of financial institutions have found this to be a difficult balance to strike at a practical level. We see the transposition of this Directive as an important opportunity to further clarify issues for these designated entities. In the past there has been confusion among entities in relation to their Money Laundering obligations. In some cases this resulted in an over-reliance on money laundering obligations in a range of inappropriate circumstances to justify requests for personal data. We have received complaints from members of the public about the collection of excessive amounts of personal data, inappropriately justified as required for anti-money laundering obligations. In other cases, documentation provided legitimately for money laundering compliance purposes is used for further, unacceptable purposes.

My Office strongly recommends that, upon enactment, every effort should be made to develop sectoral guidelines (which are provided for in the draft Bill) to clearly set out the requirements taking full account of data protection principles. We are available to provide further advice if this is helpful.

## **DNA Bill**

My Office was invited on two occasions during 2009 to provide observations on the development of the provisions of the Criminal Justice (Forensic Evidence and DNA Database System) Bill 2009. The establishment of a DNA Database raises significant issues of data protection as well as broader issues of civil liberties. While I acknowledge the potential of a DNA database to become an effective crime control resource, it is also necessary to take account of the potential human rights impact of the proposed legislation. From a data protection perspective, the provisions in relation to the retention and sharing of DNA information are particularly important. In considering the draft provisions, my Office had regard to the judgement of the European Court of Human Rights (ECHR) in the case of *S. and Marper v the United Kingdom* on 4 December 2008.

The ECHR found, in this case, that the blanket and indiscriminate retention of fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences failed to strike a fair balance between the public interest in the detection of crime and the right to respect for private life. Blanket and indiscriminate retention was found to constitute a disproportionate interference with the applicants' right to respect for private life and could not be regarded as necessary in a democratic society. The Court concluded unanimously that there had been a violation of Article 8 of the European Convention on Human Rights (right to privacy) in this case.

The Criminal Justice (Forensic Evidence and DNA Database System) Bill 2009 (published early in 2010) had to be reviewed in light of this landmark decision. This Office's submissions focussed on the implications of the Marper Judgement and the need to fully incorporate them into the legislation. The submission focused in particular on the compatibility with the Judgment of the proposed retention of the DNA samples and profiles of persons not found guilty of an offence.

## **Spent Convictions Bill**

My Office was originally approached during 2008 for observations in relation to a Private Members' Bill - Spent Convictions Bill 2007. During 2009 we reviewed the latest version of the Bill adopted by the Government (Spent Convictions Bill 2007)

and provided further comments for consideration. We welcome being consulted in regard to this important issue from both a data protection and human rights perspective. Ireland is one of a small number of EU Member States without substantive legislation in place providing for the spending of certain convictions after a stated period of time. The lack of legislation in this area has been a specific concern of this Office for a significant period of time given the requirement of the Data Protection Directive to set retention periods for personal data. The lack of set retention periods places persons convicted here, sometimes of minor offences a long time ago, in an unfavourable position in comparison to persons convicted of the same offences in other EU member states.

### **NRA/eFlow**

The operation of the M50 Barrier-Free Tolling Project continued to generate queries to my Office during 2009. I dealt with this matter in last year's Annual Report when I indicated that our engagement with the NRA had not yet been finalised.

The key issue that had remained unresolved was the setting of an appropriate period to retain motorists personal data to allow for the appropriate toll to be paid. This Office was keen to ensure that, in so far as it was possible, the right to anonymous travel across the M50 should be maintained. That said, my Office acknowledged that the NRA faced considerable practical issues in relation to deleting the personal data of motorists at an early date as desired by this Office. This was due to the large number of payment queries that arose in the early stages of the project. Our engagement on outstanding issues intensified in early 2009. It was agreed that we would carry out an audit of BetEire Flow Ltd, which administers the E-Flow scheme on behalf of the National Roads Authority (NRA). The audit gave us the information we needed to more fully assess the data processing needs of this type of operation.

Following the audit and a series of further engagements with the NRA, we agreed the following steps with the NRA:

#### Data deletion policy and procedure

For those motorists for whom the privacy of their journeys across the M50 is paramount, the NRA agreed to introduce a procedure to allow them to request the deletion of their personal data (in return, the motorist will have to agree to certain conditions, including waiving their right to query transactions). Implementation is expected during 2010. The NRA also indicated a willingness to consider the feasibility of a new form of tag product that would address some of the same concerns.

#### Retention Periods generally

My Office is working with the NRA/BetEire Flow to amend the unregistered payment process to take certain data protection concerns into account while allowing motorists to access their outstanding balance when paying their toll. Once this is implemented, the NRA intends to reduce the retention period to six months for both unregistered and registered users (with the exception of those who have not paid the relevant toll charges). In line with its obligations under the Data Protection Acts, the NRA has also undertaken to continue to keep the retention period under review.

While the issues outlined above took quite a lengthy period to resolve (given the unique nature of the system) I nonetheless consider that this is a good example of effectively accommodating data protection requirements in a complex system.

### **Health Information Bill**

In my 2008 report I noted a proliferation of uses for the PPSN (Personal Public Service Number) in the health sector which had come to our attention through our engagements with that sector. This position was further supported during 2009 through a number of engagements with different parts of the health system that also indicated that the PPSN was being used as an identifier. My Office once again availed of every opportunity during 2009 to highlight our serious concerns as to the suitability of the PPSN as a national Unique Health Identifier (UHI). I also noted that HIQA's report on the UHI for individuals also reached the conclusion, on a number of grounds, that the PPSN is not fit for purpose as a UHI.<sup>6</sup>

---

<sup>6</sup> [http://www.hiqa.ie/media/pdfs/Unique\\_Health\\_Identifier\\_Report.pdf](http://www.hiqa.ie/media/pdfs/Unique_Health_Identifier_Report.pdf)

A positive development in relation to the management and use of health information in this country is the intention of the Department of Health and Children to bring forward a comprehensive Health Information Bill which will provide a specific legal basis for intended uses of health information while at the same time safeguarding patient privacy. I very much welcome the intentions of the Department in this area and although the Bill is not yet published, it appears that my Office may be conferred with a number of additional responsibilities upon enactment. We look forward to working further with the Department of Health and Children in relation to these responsibilities. Our continuing approach will be to seek an acceptable balance between the need for health care providers to share personal health information for the care of patients and patients' right to control the use of their personal information.

### **Health Audit Networks**

My Office received queries from a number of units within different health facilities during 2009 requesting advice in relation to their proposed participation in UK-based health audit networks. This participation involved the transfer of what could be considered as patient identifiable information to a clinical audit database regarding all admissions to a particular unit to allow comparison with UK benchmarks in relation to outcomes, processes and structures to facilitate future planning and research.

Under Section 60 of the UK Health and Social Care Act 2001 approval may be granted in respect of certain projects which process patient identifiable information where patient consent has not been obtained and there is no other reliable basis in law to permit the disclosure and use of identifiable patient information. Currently there is no 'Section 60' equivalent in this jurisdiction, therefore the transfer of patient identifiable information in such circumstances would require the express consent of the patients. We have previously addressed the use of health data for clinical audit purposes in our 2007 Guidance Note on Research in the Health Sector.

As part of our consideration of these queries, we explored numerous options for rendering the data anonymous in advance of transmission to audit databases. This demonstrates the ongoing willingness of this Office to explore all possible solutions that achieve the objectives of the data controllers while also ensuring compliance with

the Data Protection Acts. In all cases a successful solution to meet all concerns was identified.

### **Engagement with Ethics Committees**

I appreciated that my Office was approached during the year to participate in the finalisation of a draft Common Application Form for persons or entities applying for ethical approval to Ethics Committees in various hospitals and HSE areas. The process which was convened by Molecular Medicine Ireland was intended to assist in streamlining the process for researchers applying for ethical approval to Research Ethics Committees. It provided a key opportunity for my Office to assist Ethics Committees to highlight to applicants for ethical approval what the key data protection requirements are for any work with personal data for research purposes. A pilot of the new application form will now be put in place across selected hospitals and I look forward to continuing to work on this important initiative.

### **Communications (Retention of Data) Bill 2009**

This Bill, which was going through the Oireachtas at the end of the year, updates the data retention provisions in the Criminal Justice (Terrorist Offences) Act 2005 and aligns Irish law with the requirements of EU Directive 2006/24/EC. It requires telecommunications companies to retain customer call data and to make this available to designated State authorities on request. In our observations on the Bill, we repeated our concerns about the adequacy of the oversight regime, the length of time during which data would be retained and the fact that the right to access data was being granted to the Revenue Commissioners as well as to An Garda Síochána and the Defence Forces.

### **ePrivacy Directive**

2009 saw the revision of the 2002 Directive on Privacy and Electronic Communications (2002/58/EC). The revision has a number of important new features which will have to be transposed into Irish law not later than June 2011. One such feature is an obligation to notify supervisory authorities and subscribers where there

has been a breach of security in relation to personal data. The EU Commission has committed to examining the case for an extension of this requirement to other sectors.

### **Google Street View**

In the course of 2009, Google began to film streets in different parts of the country to add street-level imagery to its Google Maps product. This process inevitably involved the capture of images of identifiable individuals and of other forms of personal data. The Office had a number of engagements with Google to confirm that the system would operate in accordance with data protection law. The undertakings given by Google included that advance publicity would be given to the filming and that any reasonable objections to filming would be respected. Google also confirmed that it would adopt its standard practices of blurring faces and vehicle number-plates and of providing a facility whereby any individual could secure the removal of images related to them. Google also indicated that images that were not blurred would not be retained for more than a year after these images went "live".

### ***International Responsibilities***

#### **Article 29 Working Party**

During the year, the Office maintained its active involvement with the Article 29 Working Party. The Working Party acts as an adviser and advocate when data protection issues arise at European level. It promotes a uniform application of the provisions of the EU Data Protection Directive 95/46/EC throughout the European Economic Area.

The Working Party delivered Opinions on online social networking and on the protection of children's personal data. It also gave its views on the draft revised ePrivacy Directive, the World Anti-Doping Agency draft International Standard for the Protection of Privacy, new standard contractual clauses for the transfer of personal data to processors established in third countries, pre-trial discovery for cross border civil litigation, purchases in duty-free shops and the processing of personal data by credit bureaus. The Working Party also made a contribution to the consultation launched by the EU Commission on the future of the EU's data protection regime.

All of these documents are available on the Working Party's website ([http://ec.europa.eu/justice\\_home/fsj/privacy/workinggroup/wpdocs/2009\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm)).

### **International Data Transfers**

2009 saw further progress in facilitating multinational companies to safely transfer personal data outside of the European Economic Area. By the end of the year, the Article 29 Working Party had recommended to the EU commission that Israel and Uruguay should be added to the list of countries whose systems for the protection of personal data were deemed to be "adequate". The Working Party had also commented favourably on a new, more business-friendly set of standard contractual clauses for the transfer of personal data to processors established in third countries. There was also further progress in the development of the system of "Binding Corporate Rules" (BCRs). BCRs allow the composite legal entities of a corporation (or conglomerate) to jointly sign up to common data processing standards that are compatible with EU data protection law. If they use BCRs, companies do not need individual contracts between EU and non-EU subsidiaries for the transfer of personal data between them. A number of BCRs were approved during the year and further material was published on the Working Party's website, designed to make the system more user-friendly for companies.

### **Towards new Data Protection Standards?**

The 2009 Spring Conference of European Data Protection Authorities was hosted in Edinburgh by the United Kingdom's data protection authority (ICO). The Conference focussed on an examination of the strengths and weaknesses of the current EU data protection regime, based on a study commissioned by the ICO. This was followed by a conference hosted by the EU Commission and the launch of a public consultation on new challenges for personal data protection. In its communication - 'An Area of Freedom, Security and Justice serving the Citizen' - the Commission stated that the EU "must establish a comprehensive personal data protection scheme covering all areas of EU competence" and that the EU "must be a driving force behind the development and promotion of international standards for personal data protection".

The 31st International Conference of Data Protection and Privacy Commissioners was hosted this year in Madrid by the Spanish data protection authority. A major achievement of the Conference and of its host was the approval of a "Draft of International Standards on the protection of Privacy with regard to the processing of Personal Data":

[https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/31\\_conferencia\\_internacional/estandares\\_resolucion\\_madrid\\_en.pdf](https://www.agpd.es/portalweb/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf)

The Draft drew on existing standards developed by the EU, the Council of Europe, the OECD and APEC (Asia-Pacific countries). It should serve as a template for future work in developing a harmonised international approach to data protection.

### **Personal Data Accountability**

The principle that organisations should be held accountable for the personal data that they gather and process is a key feature of data protection. Such accountability is also expected of organisations when they transfer personal data internationally. Accountability, and how an organisation can apply and demonstrate it in practice, is likely to become even more significant in the future. In the course of the year, my Office facilitated a project led by the US-based Centre for Information Policy Leadership which further explored this theme. The resulting discussion paper<sup>7</sup> was the fruit of two meetings held in Dublin involving representatives from industry, data protection authorities, academia and NGOs. A second phase of the project is due to take place in 2010, facilitated by our French data protection colleagues (CNIL).

### **Third Pillar Groups**

Though the entry into force of the Lisbon Treaty abolished the pillar structure of the European Union, the advisory role of the Article 29 Working Party is still focused on economic, social and environmental matters. The Office is also represented at meetings of groups dealing with European cooperation in the fight against crime. These groups 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

---

<sup>7</sup> [http://www.huntonfiles.com/files/webupload/CIPL\\_Galway\\_Accountability\\_Paper.pdf](http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf)

ensures that personal data within the European Customs Information System is processed in a manner that respects individual data protection rights) and the EUROJUST Joint Supervisory Body (which meets in the Hague to ensure that cross-border cooperation between EU judicial and prosecution authorities respects data protection rights).

Over the past year, these and related groups have dealt with issues such as:

- The entry into force of the Lisbon Treaty and of the Framework Decision on Data Protection in EU Police and Judicial Cooperation. The EU's data protection authorities explored the implications of these developments to develop the best strategies for continuing to uphold the data protection rights of people living and working in the European Union.
- European Commission proposals to allow law enforcement authorities access to the EURODAC system (the EURODAC system is intended to allow EU member states to compare fingerprints of asylum seekers and illegal immigrants, so that the EU's immigration and asylum functions can be properly administered). Under conditions set out in the proposals, the personal data in the EURODAC system would be used for the prevention and investigation of terrorist and other serious offences. The EU's data protection authorities drew attention to the need to ensure that such proposals were legitimate given the privacy rights of innocent people.
- The implementation of an EU Council Decision incorporating the Prüm Convention into EU law. The Decision provides a legal basis for member states to grant each other access to their automated DNA and fingerprint identification systems and vehicle registration data. The EU's data protection authorities worked to ensure that implementation by member states took place in accordance with the terms set out in the Council Decision.

## **Administration**

### **Running Costs**

The costs of running the Office in 2009 were as follows:

	<b>2008 (€)</b>	<b>2009 (€)</b>	<b>% change</b>
Overall running costs	2,041,097	1,814,553	11% decrease
Receipts	591,421	576,616	2.5% decrease

**Table 3 - Running costs**

A fuller account of income and expenditure in 2009 is provided in Appendix 3.

## Part 2

### **Case Studies**

Case study 1: Disclosure of personal data due to inappropriate security measures .....	40
Case study 2: Prosecution of Jackie Skelly Fitness for unsolicited marketing text messages .....	42
Case study 3: Disclosure of personal details by a local authority on its website.	43
Case study 4: Alleged disclosure of credit card details by a booking agent.....	46
Case study 5: Harvesting of mobile numbers from a website for the sending of marketing text messages .....	48
Case study 6: Email marketing error causes data protection breach .....	50
Case study 7: Recruitment companies sharing CVs .....	52
Case study 8: Excessive data sought on penalty points .....	54
Case study 9: Further processing personal data without consent .....	56
Case study 10: Mobile network operator fails to suppress customer marketing preferences .....	58
Case study 11: Car dealership breaks the law by sending direct marketing text messages .....	60
Case study 12: Paternity test result sent to the wrong address .....	62
Case study 13: Use of postcards to communicate with customers regarding overdue account .....	64
Case study 14: Employer breaches Acts by covert surveillance using a private investigator.....	66
Case study 15: Prosecution for sending unsolicited marketing faxes.....	68
Case study 16: Prosecution of Brasserie Sixty6 for the sending of unsolicited direct marketing text messages .....	69

### **Case study 1: Disclosure of personal data due to inappropriate security measures**

In August 2008, I received a complaint regarding the alleged disclosure of personal information by an airline. The complainant to my Office stated that in June 2008, in response to a phone call, the airline disclosed by email a travel itinerary for herself and her husband to her husband's employer and on foot of this disclosure, her husband was dismissed from his employment. The complainant stated that her husband's employer had made a written statement to the effect that the email in question was disclosed by the airline on the provision of a surname only. A copy of this statement was provided to my Office.

In the course of this investigation, the airline informed my Office that security questions were asked prior to the email in question being issued to the third party. It did not dispute that it sent the email. However, as the airline did not record the telephone call requesting the information, nor were its security questions system prompted and logged, it was not able to provide any evidence to prove that the appropriate security questions were asked in this instance. My Office also took into consideration that the booking was made from the complainant's own computer using a personal email address rather than from an email address at her husband's workplace.

On the basis of the information presented, together with the fact that the airline could not provide evidence that its own security measures were in fact used on this occasion, I arrived at the decision, following the investigation of this complaint, that the airline had contravened Section 2(1)(c)(ii) by further processing the complainant's personal data and that of her husband when it disclosed to her husband's employer their travel itinerary in an email. It also contravened Section 2(1)(d) by failing to have in place appropriate security measures to prevent the unauthorised disclosure of her personal information and that of her husband.

The security related issues highlighted by this complainant have been the subject of extensive engagement by this Office with the airline who, following this complaint, examined ways to enhance its security in relation to the handling of enquiries such as this.

This complaint clearly demonstrates the need for data controllers to have controls in place to prevent the disclosure of personal data. It is not sufficient to rely solely on the word of staff that they will ask the appropriate security questions in all instances, particularly in circumstances such as this where an individual deliberately seeks to obtain personal data which they are clearly not entitled to receive.

## **Case study 2: Prosecution of Jackie Skelly Fitness for unsolicited marketing text messages**

My Office received complaints from two individuals regarding unsolicited marketing text messages which they received in the spring of 2008 from Map Dance Limited, trading as Jackie Skelly Fitness. One complainant was a former customer of Jackie Skelly Fitness and the other was an existing customer. Both complainants informed me that they had not consented to receiving marketing text messages from this company. Furthermore, the marketing text messages did not contain an opt-out facility as required.

As part of my Office's investigation into the matter, we sought the traffic records from the third party company used to send the messages on behalf of Jackie Skelly Fitness to the complainants' mobile phones. We did this to confirm that the messages were sent by Jackie Skelly Fitness and to establish the content of those messages.

The traffic records which we obtained showed that Jackie Skelly Fitness had sent the marketing text messages in question and that the messages did not contain an opt-out facility as required by the regulations in Statutory Instrument 535 of 2003. Following my Office's investigation, I was satisfied that offences had been committed and I decided to exercise my powers to prosecute Jackie Skelly Fitness in respect of those offences.

In April 2009, at Dublin Metropolitan District Court, Jackie Skelly Fitness pleaded guilty in respect of one charge related to the sending of an unsolicited marketing text message to a customer without consent, in contravention of Regulation 13(1)(b) of S.I. 535 of 2003. The Court recorded a conviction and it imposed a fine of €1,750. Jackie Skelly Fitness also pleaded guilty in respect of one charge related to the sending of a marketing text message to a former customer which did not contain a valid address to which the recipient could send an opt-out request, in contravention of Regulation 13(8) of S.I. 535 of 2003. The Court recorded a conviction and imposed a fine of €1,500. This was the first occasion on which a conviction was recorded in respect of an offence under Regulation 13(8) for failure to include an opt-out facility in a marketing text message.

### **Case study 3: Disclosure of personal details by a local authority on its website**

I received a complaint from a member of the public towards the end of 2008 regarding the disclosure of personal data submitted as part of an application for planning permission to a local authority.

#### Background

(i) In the latter part of 2006, my Office entered into discussions with the Department of the Environment, Heritage and Local Government in an effort to establish an appropriate balance between an open and transparent planning system and the rights of individuals to privacy and data protection. Following these discussions, the Minister for Environment, Heritage and Local Government signed the Planning and Development Regulations 2007 (SI 135 of 2007). Amongst other things, these regulations introduced an amended planning application form. The amended form re-arranged the address/contact details section from the front of the form to a detachable page at the rear of the form to ensure that these personal details could be removed prior to the publishing of planning applications on the planning authority's website.

(ii) The Department of the Environment, Heritage and Local Government also issued Development Management Guidelines for planning authorities which, among other things, recommended the use of a Robots Exclusion Protocol (this is a simple protocol that, when placed on a web page, reputable search engines do not then proceed to index the page for inclusion in search results) by all planning authorities in relation to planning application data on their website to protect personal data on those websites from search engine access.

#### Complaint

In this case, the complainant completed the planning application form and provided the planning authority with his contact details on the detachable part of the form. However, the information supplied in this section was subsequently made available to the public on the local authority's website.

My Office contacted the local authority involved and asked it for its comments on what led to the publication of the contact details on the website and if it had

implemented a Robots Exclusion Protocol to prevent personal data appearing on search engines.

In reply, the local authority informed my Office that, on this occasion, its procedures which it had in place to comply with the data protection requirements did not operate and that as the procedures were relatively new, the physical removal of the contact details portion of the planning application form was overlooked. It also indicated that the procedures had since been strengthened to ensure compliance with the data protection requirements. The response also indicated that the local authority had not yet implemented a Robots Exclusion Protocol and that it was currently being considered. At that point, my Office made it clear to the local authority that, given the passage of time since the Department had published its Development Management Guidelines in 2007, we found it unacceptable that a Robots Exclusion Protocol had not yet been put in place. We pointed out that by not having it in place personal information of individuals making planning applications continued to be at risk of being picked up by search engines when the applications were uploaded onto the websites. The local authority was instructed by my Office to put in place a Robots Exclusion Protocol immediately and failing that, I would use whatever legal powers I deemed necessary to protect the personal data of those individuals who submit planning applications to that local authority. My Office subsequently received confirmation from the local authority that a Robots Exclusion Protocol had been put in place.

The complainant in this case requested a formal decision under Section 10 of the Acts. My decision found that the local authority had contravened Section 2(1)(d) of the Data Protection Acts when it published, on its website, the contact details which the planning applicant had submitted on part of the planning application form. It breached this requirement by not having in place appropriate measures to prevent the unauthorised disclosure of the planning applicant's contact details.

This case demonstrates the need for local authorities to be extra vigilant when uploading planning applications to their websites to ensure that only the information required by law to be made publicly available is published in this way. In addition,

having a Robots Exclusion Protocol or similar in place guards against the risk of the planning applications themselves being captured by search engines.

#### **Case study 4: Alleged disclosure of credit card details by a booking agent**

In January 2009 I received a complaint regarding the alleged disclosure of personal information by an internet booking agent. The complainant informed my Office that, when booking a hotel with the booking agent, he provided his credit card details to pay a deposit. However, after his subsequent stay at the hotel and having paid the bill, he received a phone call from the hotel to inform him that the bill had been undercharged by €200 in error. The complainant alleged that the hotel then contacted the booking agent who in turn provided the hotel with his credit card details and that these details were used by the hotel to debit €200 from his credit card account.

My Office contacted the booking agent in question and asked where on its terms and conditions did it state that an individual's credit card details would be shared with the hotel booked by the customer.

The booking agent, as part of its response, provided my Office with a copy of the full terms and conditions associated with the use of its website. The terms and conditions clearly state that no reservation contract exists between the customer and the booking agent and that the contract is between the customer and the hotel. The booking agent acts as a facilitator for the hotel and all rooms, availability, pricing and descriptions on hotel websites and all websites using the booking agent's technology are under the control of the hotel

In this case, the complainant, when using the booking agent to book the hotel, was actually booking directly with the hotel and not with the agent. Therefore, when he provided the credit card details on-line to pay the deposit for the hotel, the details were provided directly to the hotel and not to the booking agent as he had previously thought. Therefore, no actual disclosure to a third party took place.

Since my Office raised this issue with the booking agent, it has expanded its terms and conditions to ensure that individuals using the booking agent's website to book hotels fully understand that the credit card details provided by them are provided to the hotel.

This case clearly demonstrates how important it is for individuals to be fully aware of the terms and conditions associated with any contract they enter into. In most cases, the terms and conditions also outline how the information provided by an individual will be used. In this case, had the complainant read the terms and conditions in full, he would have been aware that the contract existed between himself and the hotel and therefore, in entering his credit card details on-line, he was supplying them to the hotel. I can fully accept, however, that terms and conditions are not always either immediately available or accessible in terms of language to a person seeking to make a booking over the internet.

### **Case study 5: Harvesting of mobile numbers from a website for the sending of marketing text messages**

In January 2009 an individual complained to me regarding his receipt of an unsolicited marketing text message. The complainant stated that he had placed his number on a website to advertise a property he had available to rent. He subsequently received a text message from an energy efficiency testing company offering its services to him. He was concerned not only about the way his number was obtained and processed by the company, but also by the fact that there was no 'opt out' option included in the message he received which would have allowed him to object to receiving any further communications.

In order to legitimately contact an individual mobile phone subscriber by text message for direct marketing, the sender must have obtained prior consent from the individual. Otherwise the marketer runs the risk of committing a criminal offence under Regulation 13(1)(b) of S.I. 535 of 2003 (as amended), and may be prosecuted. The failure of a sender to include a cost free opt out in a marketing text message is also an offence liable to prosecution.

My Office commenced an investigation into the matters raised by the complainant. We contacted the company to seek an explanation and provided it with a copy of our Guidance Note on the use of electronic mail for direct marketing purposes to assist it in responding on the matter.

The company responded by admitting that it did source the complainant's number from a website and that it proceeded to then send him a marketing text message regarding a service it was providing to home owners. It was extremely apologetic for causing offence to the complainant and for breaking any regulations. It explained that it had recently commenced offering the service. It also confirmed that it had abandoned plans to continue with such marketing and it advised that the complainant's personal details were now deleted from its databases.

As an act of good faith and in an effort to amicably resolve the matter to the satisfaction of the complainant, the company donated a sum of €100 to a charity of the complainant's choice. The complainant was satisfied with this outcome.

This case is an example of the disturbing trend of commercial entities sourcing mobile numbers of private individuals from websites or from other published sources for the purpose of using those numbers to market their own products. Any person who advertises their property for sale or rent on a website or elsewhere should not, as a consequence, be exposed to the risk of receiving unsolicited text messages from a company promoting its own products.

### **Case study 6: Email marketing error causes data protection breach**

In September of 2008 four complaints were received by my Office regarding the sending of a marketing email by a company, in which the email addresses were visible to each of the recipients. The complainants also advised that they had not consented to receiving the email in question. It was also brought to my attention that the email did not contain an 'unsubscribe' option which would have enabled the recipients to record their preferences not to receive any further marketing communications. It was also a matter of concern to me that one of the complainants advised me that he had previously contacted the company to request removal of his email address, and despite that, he subsequently received the email which was the subject of the complaints to my Office.

The company notified me, following its own receipt of a complaint, that it had sent a marketing email which contained 1400 email addresses. These addresses were disclosed in the carbon copy field (cc) in error, as opposed to listing the addresses in the blind carbon copy field (bcc), which would have ensured that the personal email addresses of the individual recipients would not have been visible. Once it had realised the error, the company advised me that it recalled all the emails and shut down its server. However, as the complaints to my Office raised a number of other concerns regarding the electronic marketing practices of this company, I decided that an investigation of the matters raised by the complainants was warranted.

In the investigation of these complaints, my Office sought an explanation from the company as to why it sent the marketing email to the recipients without their consent and without the inclusion of a cost free opt out facility. The company responded that one of its databases was used in error. It explained that a new member of staff used an old database of consumer enquiries in error and also failed to protect the email address details of the individual contacts on the database. Furthermore, the company did not have sufficient monitoring of its email marketing to provide an opt-out at the point of collection of contact details or to unsubscribe recipients effectively when requested to do so. Following my examination of the response from the company, I was satisfied that it had committed offences by sending the unsolicited email to the

recipients without their consent and also without including an unsubscribe option in the email.

On foot of the four complaints to my Office, and in an effort to correct the deficiencies in its marketing operations, the company retained the services of a specialist digital communication service provider to manage its databases and email activity to ensure that there could be no recurrence of these issues in the future. The company also strengthened its policy around database use and it introduced a new anti-spam policy. As a gesture of goodwill, it offered the complainants free passes to an upcoming social event and a letter of apology for the inconvenience caused to them. Furthermore, it also made a charitable donation of €500 to a well-known charity. The four complainants were satisfied to resolve their complaints on that basis. Given that this company had not come to my attention before, I was satisfied that a prosecution against the company was not warranted at that time based on my normal policy in such matters. I am happy to report that my Office has received no further complaints regarding the company's marketing practices since the investigation of these complaints.

### **Case study 7: Recruitment companies sharing CVs**

In April 2009 I received a complaint against a recruitment company (company A) regarding an alleged disclosure of the complainant's curriculum vitae (CV) to another recruitment company (company B). The complainant submitted his CV to company A for a particular job which was advertised on a recruitment website. However, he was subsequently contacted by company B asking for further details in relation to his CV. In a phone call, company B confirmed to the complainant that it had received his CV from company A. The complainant claimed that the company to whom he sent his CV did not obtain his consent to disclose his CV to another company.

My Office commenced an investigation into the matter and we wrote to company A and asked it to demonstrate the consent it considered it had in place to disclose the complainant's CV to company B. A key principle of data protection is that personal data should be used and disclosed only in ways compatible with the purposes for which it was obtained. Company A explained that it and company B, although they were separate legal entities and registered separately with the Companies Registration Office, were effectively run as one company. They both shared, among other things, the same office space, databases, IT infrastructure, telephone system and management. However, one of the companies handled recruitment of middle and senior management while the other one handled recruitment of office and customer support staff. In this case, when the complainant submitted his CV to Company A, the consultant who received it passed it to a consultant in Company B as possible skills were identified from the CV which may have been of interest to the other consultant's clients.

My Office advised Company A that the companies were two separate entities and therefore, individuals using the services of either one should be made fully aware, prior to submitting their personal information, that it would be shared between the two companies. We also noted that the privacy policy on its website did not contain any reference to the fact that both companies share information and we advised that it should contain a statement which informed individuals using the website how their information would be processed and that their information would be shared between the two companies. My Office also advised that, if it was unable to do this, the only

alternative was to separate out the two entities completely and cease sharing personal information.

As a result of our investigation, we received an assurance from Company A that it would insert a statement on both of the companies' websites to inform individuals using the websites how their personal information would be processed and of the fact that it would be shared between both companies. It also indicated that it would no longer have separate entities and that, although this would take some time to arrange, both companies would trade as one company in future.

I welcome the fact that the data controller immediately put in place the measures needed to bring it into compliance with the Acts. It is important for any data controller to make individuals fully aware at the outset as to how their personal data will be processed and to whom it may be disclosed. As a general rule personal data may not be shared between two legal entities without the consent of the individual about whom the data relates.

### **Case study 8: Excessive data sought on penalty points**

In November 2008, my Office received a complaint against Quinn Direct Insurance regarding the amount of information sought when an individual requested a quotation for motor insurance. The complainant stated that, during a phone call to Quinn Direct Insurance in November 2008, in which he sought a quotation for motor insurance, he was asked for information on any penalty points he had received on his driving licence during the previous five years.

Section 2(1)(c)(iii) of the Data Protection Acts, 1988 and 2003 provides that personal data obtained by a data controller shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are collected or are further processed. In October 2002, the Minister for Transport announced the introduction of penalty points for speeding offences for all drivers under the Road Traffic Act, 2002. Other offences were added to the penalty points system since then. Under the Act, penalty points remain on a person's driving licence for a period of three years.

My Office contacted Quinn Direct Insurance and raised our concerns that potential customers for car insurance were being asked to provide details of penalty points for the previous five years while the applicable legislation states that such details should be kept on a driver's licence for only three years. Quinn Direct Insurance responded to my Office stating "In underwriting a motor policy, and assessing the risk involved, we require information from the proposer on the convictions and or penalty points obtained on their licence in the previous five years. The risk may be assessed differently depending on the offence type, the number of points and whether or not there was a driving ban imposed - for example, the rating for careless driving will be different to speeding. We do not rate solely on the number of points but require this information in deciding on the severity of the offence for assessing the policy."

My Office expressed its dissatisfaction at Quinn Direct Insurance's reasons for seeking information on penalty points for the previous five years in circumstances where the statutory obligation for the retention of penalty points on a driver's licence was three years. We requested that it cease the practice of seeking such data immediately. Quinn Direct Insurance in response stated that its quotation process

would be revised to ensure that details on penalty points would only be requested for the previous three years rather than five years as had previously been the case.

This case clearly demonstrates how important it is that data controllers satisfy themselves, on an ongoing basis, that information sought from customers is not excessive. Unless there is a clear basis for requesting certain categories of personal data, data controllers should exercise restraint when seeking personal data and they should ensure that only the minimum amount of personal data necessary is processed. This is particularly the case where the data sought relates to matters such as offences.

### **Case study 9: Further processing personal data without consent**

My Office received a complaint in December 2008 from a data subject regarding the alleged use of video clips of her and her family for training purposes, without her consent, by the HSE West. The video clips were recorded with the data subject's consent as part of her family's participation in a particular programme known as Marte Meo. The data subject's family had agreed to participate in the programme for the purpose of being a foster family. The data subject informed my Office that she first became aware that video clips concerning her family's participation in the programme had been shown at a conference held in Germany when her Fostering Social Worker telephoned her after the event to give her feedback from the conference.

According to the HSE, the Marte Meo model is used by Social Work Teams at the HSE as a supportive intervention in fostering cases. It is a film-based intervention used to provide feedback to the prospective foster family on their natural supportive communications and how these can support their preparation for a foster placement. In this case the data subject's family were asked by the HSE West to provide care to two young girls in an emergency situation.

The HSE West informed my Office that the data subject's Fostering Social Worker understood that the data subject had given verbal consent for the use of the video clips by her supervisor at the conference. The HSE West confirmed to my Office that two short video clips of the fostering video tape were used at the conference. The HSE West also confirmed that when the proposal to use the video clips was first put to the data subject she was informed that a signed consent would be sought. However, on a subsequent visit to the data subject's home, the Fostering Social Worker forgot to bring the consent form. The HSE West proceeded to use the video clips even though it had not obtained the written consent of the data subject and her family.

My Office informed the HSE West of our view that it had breached the Acts by further processing the video clips without obtaining the consent of the data subject and her family. My Office also informed the HSE West that, based on information

provided by them, the breach occurred when the HSE West departed from its own procedures - i.e. it failed to obtain written consent.

My Office's approach to complaints is to try to reach an amicable resolution. The HSE West confirmed its willingness to acknowledge its error and to apologise in writing to the data subject. It also informed us that a system was now in place to ensure that all consent forms are completed according to the Marte Meo standards. The data subject accepted the amicable resolution of her complaint.

This case study demonstrates how an organisation can breach the Acts when its staff, however well-intentioned, fail to follow internal procedures. It also highlights the importance of staff training in data protection.

### **Case study 10: Mobile network operator fails to suppress customer marketing preferences**

In the Spring of 2009 I received complaints from two customers of a mobile network operator (MNO) about the difficulties they were experiencing when attempting to register their preference to opt out of further direct marketing from their MNO. The difficulties experienced resulted in them receiving further marketing emails, despite indicating to the MNO that they had amended their marketing preferences and opted out. Both individuals informed me that they had made a number of attempts to opt out, including updating their account preferences, and clicking on the unsubscribe link contained in the marketing emails. The first complainant further informed me that he had communicated with the MNO through the 'contact us' facility on its website and he subsequently received a telephone call from a representative who confirmed that his details would be removed from all circulation lists. Unfortunately he continued to receive further marketing email.

When my Office contacted the MNO, we were told that in the cases of both complainants, they had provided their email addresses in the context of signing up to its services and neither individual availed of the opportunity given at that time to opt out of email marketing. However, it acknowledged that when both complainants tried to unsubscribe by clicking on a link in the email they received, an error occurred in the server used by the company's data processor to operate the suppression facility, with the result that the marketing preferences of both individuals were not updated to reflect their preferences. Furthermore, it advised us that due to an administrative error, both complainants' email addresses were selected as part of a marketing campaign and they received an unsolicited marketing email promoting the company's newsletter. Regarding the first complainant, the company identified a lag period of up to four weeks between the period that the complainant had the conversation with the call centre representative requesting suppression, and the time that his email address was selected from the system for inclusion in the marketing campaign. The MNO acknowledged that this was unacceptable. However, the company informed us that it had addressed this and had taken steps to ensure that marketing preference changes are recorded and updated in a period of no more than forty eight hours.

As a means of ensuring that issues such as those highlighted in these complaints did not occur again, the company informed us that it was developing an E-learning data protection training programme for all employees which would include a module on the requirements for compiling marketing lists and correctly operating marketing campaigns. In the interim, it would provide updated guidance sessions to its direct marketing personnel. It also assured us that the technical error in the server used by the company's data processor was a once-off isolated incident and that steps had been taken to mitigate against this occurrence in the future. The company also said that it sincerely regretted that both customers did not receive the high level of customer service that it strives to achieve in the observance of its customers' marketing preferences and it assured my Office that neither individual would receive any further marketing communications from the company. As a gesture of goodwill for any inconvenience caused to both individuals, the company offered each of them an ex gratia payment of €150 and it extended its apologies to them.

When contacted by my Office, both complainants were happy that the issues raised in their complaints had been dealt with satisfactorily and they accepted the goodwill gesture and apology from the company.

Whilst I am encouraged that my Office has not received any further complaints concerning the marketing operations of that MNO, I was disappointed at the series of flaws in its marketing operations, which placed undue inconvenience on these complainants in attempting to have their marketing preferences recorded and respected. Regulation 13 of SI 535 of 2003 (as amended) is clear on the legal obligations placed on marketers who wish to obtain and use customer contact details for marketing purposes and on the further obligations imposed on marketers to provide opportunities to those customers to object to the use of their contact details for marketing communications. In line with my standard procedures in this area, the MNO was issued with a warning as these incidents constituted its first interaction with my Office in this area and any future matters will therefore be considered for prosecution.

### **Case study 11: Car dealership breaks the law by sending direct marketing text messages**

In mid 2009 I received two complaints from individuals who had received direct marketing text messages from a car dealership promoting special offer trade-ins. One of the complainants had purchased a car from the dealership in 2006, whilst the second complainant had used the dealership in 2008 for repairs. Neither individual consented to receiving direct marketing text messages from the dealership. It was also a concern to me that the messages were sent without the inclusion of a cost free facility by which the individuals could object to the use of their mobile numbers for further marketing.

As part of the investigation of these complaints, my Office contacted the dealership to obtain details, if any, of the consent it had in place to send the messages to the complainants and to find out why the messages were sent without an opt out facility. In its response, the dealership informed us that the first complainant had completed a vehicle order form on the purchase of his car, and that the form included a data protection clause which permitted it to contact the complainant in the future. However, having examined the form in question, I could find nothing to indicate that the customer had consented to future contact. The dealership also provided us with a copy of the job card regarding the repair work it had carried out on the second complainant's car. Again, following examination of it, I could find no evidence that it had obtained consent to send this individual marketing text messages.

It was clear to me that the dealership did not obtain the consent of either individual to send them marketing text messages. On the issue of the non-inclusion of an opt out facility in the two messages sent to the complainants, the dealership stated that its telephone number was included in the messages and that this was considered sufficient to let the recipient know that all they had to do to opt out was to dial that number. I do not accept that the inclusion of a telephone number in a marketing text message to inform the recipient of the number to call for the purpose of availing of the advertised offer in the text message meets the requirements of S.I. 535 of 2003 (as amended) with regard to giving the recipient a valid address to which they may send a

request that such marketing communications shall cease. Indeed I have already successfully prosecuted a company on this very issue.

In an effort to assist the dealership in achieving understanding and compliance with the legislation concerning SMS marketing, my Office sent it our Guidance Note on the use of electronic mail for direct marketing purposes. We also advised it to ensure that consent to send marketing text messages was obtained from the customer at the point when the customer provides their contact details. As a means of ensuring that no further marketing text messages would be sent by the dealership to any other individual without their consent, we requested it to delete its marketing database of mobile numbers.

Following our investigation of these complaints, the dealership informed my Office that it wished to engage in an amicable resolution process. By way of amicable resolution it offered a letter of apology to each of the complainants and it made a donation to charity. Both complainants were satisfied to have their complaints resolved on that basis. In turn, my Office warned the dealership that if its marketing operations were the subject of any further complaints to us, it was likely that prosecution action would be taken against it.

From a data protection perspective, it is critical that a marketer who wishes to engage in electronic direct marketing obtains consent from the recipient before a marketing text message is issued. Furthermore, marketers are also obliged to offer the recipient an opportunity to object to receiving further marketing text messages. This case is another example of the risks which are taken by marketers who do not take the required precautions before embarking on text message marketing campaigns.

### **Case study 12: Paternity test result sent to the wrong address**

My Office received a complaint in April 2009 from an individual concerning the disclosure of sensitive personal information by a data controller who provides paternity testing services.

The background to the complaint is that a DNA kit was ordered from the data controller, which duly arrived at the correct address, swabs were taken and the kit was returned to the data controller the next day. However, after a period of time had elapsed and as the test result was not forthcoming, the individual concerned phoned the data controller on 30th March 2009, to be informed that the test result had been posted on Friday 27th March. When the result had still not arrived the following day, the individual concerned again phoned the data controller and at that stage asked that it trace where the test result had been posted to. The data controller stated that the result had been posted to number 83 of a particular housing estate. However, the address of the individual concerned was number 82. When contact was made with the occupants of number 82 on this matter, they dropped the already opened envelope through the letter box of number 83.

My Office commenced the investigation of this complaint by informing the data controller that Section 2 of the Data Protection Acts 1988 and 2003 imposes responsibilities and obligations on data controllers regarding the collection, processing, keeping, use, disclosure and security of personal data. We also pointed out that medical data constitutes sensitive personal data under the Acts and we asked for an explanation as to how this sensitive personal information was issued to the incorrect address, despite the original DNA kit being posted to the correct address.

In its response the data controller stated that in normal circumstances addresses are printed from its system on to labels which are then placed on the envelope. On the said day, its system was not functioning properly and because of that it entered addresses manually. Due to human error, the person writing the address put the number 83 on the envelope instead of 82, despite the fact that the records held the accurate address. It said that it was confident that the error was a one-off occurrence. The data controller also conveyed its apologies to the individual concerned for any

inconvenience caused and it offered to provide a full refund of the fee involved in order to amicably resolve the matter. This offer was accepted by the individual concerned and the complaint was resolved on this basis.

This complaint illustrates the need for data controllers to be vigilant at all times with regard to the processing of personal data. While the data controller may have had an appropriate electronic system in place to ensure that letters were properly addressed to its clients, the fall-back manual processes which came into play when the electronic system was out of commission failed in this case, leading to the disclosure of sensitive personal data. While the data controller put the incident down to human error, the consequence of not having any double checking in the manual process was a disclosure of sensitive personal information and a breach of the Data Protection Acts. This breach understandably caused great upset to the affected individual whose test result was disclosed to a neighbour.

### **Case study 13: Use of postcards to communicate with customers regarding overdue account**

In July 2009 I received a complaint from a data subject concerning a company communicating with him via postcard to inform him that his account was overdue. The company communicated with him twice via a pre-printed postcard marked Urgent Overdue Account in white print on a red background. The postcards were delivered to the customer's address through the normal postal system.

The data subject pointed out to my Office that these postcards had come through the postal system and they had potentially been seen by the staff in the sorting office, the staff in the local general post office, by staff in the local post office which is in a small rural area and the postman. He also pointed out that the bright red design of the cards and the large print on them made it very easy for postal staff handling them to see and read their contents. The data subject also told my Office of the embarrassment caused to him and his wife as a result of the sending of the postcards through the postal system as the postman who delivered them was a neighbour of his.

My Office contacted the company and informed it that the sending of information on a postcard to the data subject regarding his overdue account constituted a disclosure of his personal information and that such a practice was in breach of the Data Protection Acts, 1988 and 2003. We requested that the company confirm to us that they would immediately and voluntarily cease this practice.

The company responded to my Office promptly and informed us that it had taken verbal legal advice before sending the postcards and that it was not aware that it was in breach of the Acts. It confirmed that it would immediately and voluntarily cease sending such postcards to customers whose accounts are overdue. My Office received full cooperation from the company throughout our investigation of this matter.

We attempted to arrange an amicable resolution of this complaint, as the law obliges us to do in the first instance, but our efforts in that regard did not succeed. The data subject then requested a formal decision of the Data Protection Commissioner on his complaint.

In November 2009 I issued my decision on this complaint. I informed the data subject that following my Office's investigation of his complaint I was of the opinion that the company twice contravened Section 2(1)(d) of the Data Protection Acts, 1988 and 2003 by failing to take appropriate security measures against disclosure of his personal data. These contraventions occurred when it issued two postcards to him in the postal system, each of which contained personal data.

This case demonstrates the need for data controllers to exercise great care in their handling of personal data and to refrain from actions which might compromise that data from a security perspective. While I appreciate that businesses need to pursue their customers for overdue accounts, they are obliged to comply with the law in doing so. Disclosing the fact of an overdue account on a postcard sent to a customer is a clear infringement of the Data Protection Acts and it should not happen.

On a more general level, data controllers who use postcards for whatever purpose should ensure that the message conveyed on them does not involve the processing of personal data. Convenience must not be put before security of personal data in such cases. I would strongly encourage any data controller whose practice it is to use post cards to re-examine such practices from the perspective of their legal obligations regarding security measures for the processing of personal data. The key message to be taken from this case study is 'think data security before convenience.'

### **Case study 14: Employer breaches Acts by covert surveillance using a private investigator**

In October 2008, I received a complaint from an individual concerning the processing, without his knowledge or consent, of both his and his children's personal data by his employer. The complaint involved the obtaining and processing of his personal data and that of his children by way of a private investigator producing footage of his movements and his children's movements on a DVD for the company without his knowledge or consent.

My Office commenced an investigation into the matter by writing to the company. We informed it of its obligations under the Data Protection Acts and we asked for its comments on the complaint. The company informed my Office of the circumstances which led to it hiring a private investigator to check on the employee's activities. According to it, the complainant was employed as a sales representative and, as such, spent virtually all of his time away from the company's premises. It stated it became concerned that the employee was not carrying out his duties as required by his contract of employment and it decided it was necessary to check on his activities in his sales territory. A private investigator was engaged to check on the employee's activities in order to establish whether or not he was performing his duties. The private investigator recorded the movements of the employee for a period of approximately one week and produced a DVD of those movements which he provided to the company. Some of the recordings produced on the DVD also contained images of the employee's children.

My Office remained concerned about the justification for the processing of the employee's personal data by way of the private investigator recording his movements. We asked that the company review any documentation it had which it believed may suggest that the processing of the employee's personal data in this way was justified. We subsequently received a range of documents in that regard. My Office also asked if it had taken any steps to address the concerns it had about the employee's activities prior to the hiring of the private investigator - to which it replied that it believed there were no other steps it could have taken. It also informed my Office that it felt it needed to make observations of the employee's company car over a period of at least a

week before it could be satisfied that the employee had a case to answer. The company stated that it did not have the resources internally to check this over such a period of time and for that reason the private investigator was asked to check and report. Having considered the case put forward by the company and the documentation submitted, my Office informed it that we considered that the processing of the employee's personal data by way of a private investigator recording the employee's movements was not justified as it had not taken appropriate steps to highlight its concerns to the employee prior to making the decision to hire a private investigator to record his movements. My Office also requested that the DVD in question be destroyed and we subsequently received confirmation of its destruction from the company.

The complainant subsequently requested a decision under Section 10 of the Acts. My decision found that the company had contravened Section 2(1)(a) of the Acts by the processing of the employee's personal data and that of his children, in the recording of images by a private investigator acting on its behalf, without his knowledge or consent.

Covert surveillance of individuals is very difficult to reconcile with the Data Protection Acts. As a minimum and this may not even make such surveillance legal, there must be strong and evidence based justification for such surveillance in the first instance.

## **Case study 15: Prosecution for sending unsolicited marketing faxes**

Early in 2009 I received a complaint from an individual concerning unsolicited direct marketing fax messages he had received in November 2008 and January 2009. The faxes were sent to his fax number by Prism Fax Services Ltd promoting various holiday offers, competitions, hotel offers, etc. on behalf of a number of advertisers. In support of his complaint, the complainant supplied copies of the faxes he had received.

Regulation 13(1)(a) of S.I. No. 535 of 2003 (as amended) provides that marketing faxes may not be sent to individuals without their consent.

My Office commenced an investigation by contacting Prism Fax Services Ltd. It informed us that the intended recipient of the fax messages in this case was a school. However, it said that it had entered the fax number of the school incorrectly on its database and, as a result, the faxes were sent to the wrong number. It confirmed to my Office that it had now removed the incorrect fax number from its database. I was satisfied that offences had been committed by Prism Fax Services Ltd and I decided to prosecute the company in respect of those offences arising from previous interactions with it on the sending of unsolicited faxes where the legal requirements in this area were made clear.

In December 2009, in the Dublin District Court, Prism Fax Services Ltd pleaded guilty in respect of one offence under Regulation 13(1)(a) of S.I. No. 535 of 2003 and two offences under Regulation 13(1)(a) of S.I. No. 535 of 2003 (as amended), in respect of the sending of direct marketing faxes to an individual without their consent on dates in November 2008 and January 2009. The Judge accepted the guilty pleas and Prism Fax Services Ltd was convicted and fined a total of €2,250.

This was the first occasion on which I brought prosecution proceedings for an offence in respect of the sending of unsolicited marketing fax messages. Prism co-operated fully with my Office's investigation of this matter and indicated a willingness to plead guilty at the earliest opportunity, which further assisted matters.

## **Case study 16: Prosecution of Brasserie Sixty6 for the sending of unsolicited direct marketing text messages**

In July 2008 I received complaints from members of the public regarding marketing text messages that were sent to them by a Dublin based restaurant, Brasserie Sixty6. The complainants alleged that they had not consented to the receipt of the text messages.

My Office investigated the matter as it is an offence for a marketer to send a marketing text message to an individual without prior consent. In the course of our investigation, my Office contacted Brasserie Sixty6 to ascertain what consent they had to send the messages to the individuals concerned. However, Brasserie Sixty6 was unable to provide evidence of such consent. It said that some of the telephone numbers used to make reservations had been added to the marketing text messaging field, instead of the reservation field, on its computer system due to human error. It did, however, advise that those numbers were now deleted from the marketing database.

Unfortunately, one of the individuals concerned continued to receive marketing text messages after this, as his number was not removed from the marketing database as a result of human error.

I was very surprised that Brasserie Sixty6 was the subject of complaints about marketing text messages, given that only one year earlier, in July 2007, my Office had investigated several complaints against Brasserie Sixty6 in relation to direct marketing text messages. Following an investigation of those complaints, my Office found that these complainants had provided their mobile numbers in the context of making a reservation and at no stage in the collection of the numbers was their consent sought to subsequently market them. Following the 2007 investigation, I decided, in line with my normal policy in such matters, to seek to amicably resolve those complaints and not take prosecutions, as these were first offences. By way of amicable resolution, Brasserie Sixty6 had agreed to delete the database and to review

its procedures for the collection, storing and use of mobile numbers. It also made a goodwill gesture of a voucher to each of the complainants.

In light of the 2007 investigation in relation to a similar issue, I deemed the subject matter of the 2008 complaints to be repeat offences and I therefore decided to bring a prosecution against Brasserie Sixty6 in relation to four offences which came to my attention.

My Office issued four summonses in the Dublin District Court in relation to these offences. These came before the court in June 2009. Home RBVR Limited, trading as Brasserie Sixty6, pleaded guilty to the charges. Following evidence given by my staff, the Judge recorded four convictions against Home RBVR Limited and imposed a total fine of €3,250.

## **Part 3**

### ***Guidance***

#### **Breach Notification Guidance:**

**[http://www.dataprotection.ie/docs/Breach\\_Notification\\_Guidance/901.htm](http://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm)**

#### **Direct Marketing - A General Guide for Data Controllers:**

**[http://www.dataprotection.ie/docs/DIRECT\\_MARKETING\\_-\\_A\\_GENERAL\\_GUIDE\\_FOR\\_DATA\\_CONTROLLERS/905.htm](http://www.dataprotection.ie/docs/DIRECT_MARKETING_-_A_GENERAL_GUIDE_FOR_DATA_CONTROLLERS/905.htm)**

## **Appendices**

Appendix 1 – Presentations

Appendix 2 – Registration statistics

Appendix 3 – Account of income and expenditure

## ***Appendix 1 – Presentations and Talks***

During 2009 my staff and I gave presentations to the following organisations:

### **Citizens' Advice**

Citizens' Information (Information Providers Programme)

### **Educational**

HEAnet

SLSS

Roslyn Park College

Institutes of Technology FOI Network

### **Financial Services**

Limerick/Clare Chapter of Credit Unions

ICCA

### **Other Commercial**

Irish Credit Bureau Ltd

Irish Finance Houses Association

IRISS

### **Government Agencies**

CMOD

Department of Social & Family Affairs

Public Affairs Ireland (x5)

Department of Finance

Comhairle North Western Region

IPA

### **Direct Marketing**

Irish Direct Marketing Association

Irish Internet Association

Association of Advertisers in Ireland

**Health Sector**

Royal College of Surgeons in Ireland

HSE

**Insurance Sector**

The Insurance Institute of Ireland (x5)

**International**

APEC Data Privacy Seminar, Singapore

European Data Protection Conference

World Information Technology & Services Alliance, Bermuda

**Legal**

The Law Society Corporate and Public Sector Committee

**Mixed Seminars**

Systems Administrators Guild of Ireland

PDP DP Practical Compliance Conference

Institute of International & European Affairs

ICS

Association of Compliance Officers in Ireland (x2)

Corporate Governance and Administration Conference

**Voluntary/Charity**

MABS

Special Olympics Ireland

## **Appendix 2 - REGISTRATIONS 2009**

The total number of register entries in 2009 was 4,318. This figure can be broken down into the following categories:

*(a) Financial and Credit Institutions*

540

*(b) Insurance Organisations*

442

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

78

*(d) Telecommunications/Internet access providers*

55

*(é) Health Sector*

1273

*(f) Pharmacists*

1043

*(g) Miscellaneous*

374

*(h) Data Processors*

540

**Total number of registration entries:**

<u>2007</u>	<u>2008</u>	<u>2009</u>
5699	4156	4318

In 2009 the number of organisations registered increased by 162 (approximately 4%). This increase reflects efforts to increase awareness among data controllers of their obligations under the Data Protection Acts.

**Appendix 3 - Abstract\* of Receipts and Payments in the year ended 31 December 2009**

<b>Receipts</b>	<b>2008 - €</b>	<b>2009 - €</b>
Moneys provided by the Oireachtas	2,041,097	1,814,553
Registration Fees	591,421	576,616
	<b>2,632,518</b>	<b>2,391,169</b>
<b>Payments</b>		
Staff Costs	1,399,075	1,352,133
Establishment Costs	184,460	161,737
Education & Awareness	97,712	0
Legal & Professional Fees	323,311	283,972
Incidental & Miscellaneous	36,539	16,711
	<b>2,041,097</b>	<b>1,814,553</b>
Payments of Fees to the Vote of the Office of the Minister of Justice, Equality & Law Reform	591,421	576,616
	<b>2,632,518</b>	<b>2,391,169</b>

*\*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.*