An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Twenty-Second Annual Report of the Data Protection Commissioner 2010

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

PRN. A11/0136

Contents

List of tables and figures

Part 1

Foreword

2010 was a year of continuity, change and anticipated change.

We continued to use the full "tool-kit" provided to us by law. This permitted us to deal with legitimate complaints from individuals about denial of their data protection rights. It also allowed us to work towards an improved general standard of data protection in the country – especially in the area of data security.

We operated mainly by persuasion. But we did not hesitate to use enforcement powers where there was evidence of rights being wilfully ignored.

We look forward to a strengthening of those powers arising from expected changes in domestic and EU law. This will allow us to deal more robustly with those organisations that fail to demonstrate accountability for the personal data entrusted to them.

Such failure was evident in the insurance sector. A detailed investigation of data sharing in that sector revealed serious lack of respect for the data protection rights of individuals. I am glad to report that some remedial measures have already been taken by the sector. We will continue to deploy our full "tool-kit" to ensure that compliance with the law is achieved in a sector that is a major holder of sensitive personal data.

The extent and proportionality of data sharing in the public sector has also been a source of concern. Following a successful engagement with the Department of Social Protection, supplemented by information from audits of major public sector holders of personal data, we have drawn up a set of guidelines which we expect to be adhered to by all public sector organisations. Transparency and proportionality are the key guiding principles in this area.

We continued to operate with severely limited resources. This required a strict prioritisation of activities, seeking a "multiplier effect" from all activities we engaged in. Thus, the investigation of complaints and the results of sectoral audits and

inspections led to more targeted guidance and, where necessary, specific enforcement action.

I was honoured to be re-appointed as commissioner for a further 5-year period. The key to our success remains the dedicated commitment of the Civil Service staff assigned to the Office. Whether dealing patiently with callers to our help-desk, addressing complex legal issues, or trudging through the December snow to make an unannounced inspection, they cheerfully demonstrated the very best of public service.

Billy Hawkes
Data Protection Commissioner
Portarlington, March 2011

Special Investigation

In 2010 my Office undertook its most wide ranging and comprehensive investigation of a database of personal data known as Insurance Link. I am publishing the outcome of that investigation as an Appendix to this report.

Insurance Link is a shared claims database first developed in 1987 by the insurance sector as a facility to allow member organisations to share and cross-reference their insurance claims data. Members check the system for previous claims each time an individual makes an insurance claim. If a previous claims history exists, summary details will appear in the search results. As of 12 November 2010, there were 2,441,838 claim records on Insurance Link representing details on a large part of the population.

The investigation was prompted by significant concerns on my part about the operation and legitimacy of Insurance Link and its compliance with data protection legislation. A striking outcome of the investigation was the lack of transparency with regard to Insurance Link outside of its immediate membership. The existence of a database containing information on almost two and a half million claims needs to be clearly referenced and signposted by the insurance sector to allow members of the public to easily obtain more information on Insurance Link and its functions and purposes. This is especially the case where the data in question is used to make decisions on individuals.

The investigation also found that far too many individuals in insurance companies had access to the database with little or no oversight of that access. Some serious incidents of inappropriate access were identified and are listed.

Introduction

The resources available to the Office in 2010 were significantly reduced. The challenge for us was to continue to increase our efficiency and to achieve the same or better results with the resources we have. While we have had to cut back in some areas, we have found ways of maintaining our core functions of defending privacy rights and enforcing corresponding obligations. As an example in this area, given that we don't have specialist legal staff, the proper exercising of our prosecutorial functions has heretofore required the retaining of external legal advice at all stages of our prosecutorial functions. This placed a significant strain on the financial resources of the Office. In part influenced by our reducing resources, we carried out in-depth research into the prosecutorial process. Drawing from that analysis, an internal procedures manual was produced which documents the step by step procedures to be followed for the issuing and serving of summonses. In effect, the procedures manual resulted in the creation of a series of internal templates and practices that allowed senior staff to maximise the amount of prosecutorial work that can be handled internally without the need for external legal advice, greatly reducing the financial strain on my Office in discharging our prosecutorial functions. In 2010 and subsequently, all cases have been successfully prosecuted in the District Court on the basis of the new procedures with the requirement for legal assistance reduced to the minimum – i.e. representation of the Data Protection Commissioner as prosecutor on the day itself at hearings, at a low fixed fee wherever possible.

However, there is a limit to what can be achieved with new efficiencies and prioritisation while at the same time meeting the expectations of our customers. These include large multinationals located in Ireland who have a reasonable expectation that we are suitably resourced to assist them in meeting their obligations here and beyond in the EU.

Data controllers (organisations entrusted with personal data by members of the public) carry the main responsibility for the creation of a safe environment for the processing of personal data. Our Office can only play a supportive role. Already there are signs of tension, such as a recent Irish Times poll (13 December 2010) that found that 57% of respondents considered that Ireland's data protection rules are not sufficiently robust. Obviously this is not a scientific poll, but it reflects our

experience of public concerns in this area. In a previous annual report, we asked what would happen if the public stopped trusting public and private sector organisations to gather and process their personal data. Such a loss of confidence would have very serious consequences. It is therefore in everybody's interest to retain the trust of the public that their personal data will be safeguarded. Public and private sector organisations can contribute to achieving this safe space for privacy by designing new technology and services with privacy in mind. Privacy should be built-in to systems, services and products from the beginning so that compliance with data protection regulations is seamless and automatic.

The results of a failure to take this approach are all too obvious. Aside from the list of prosecutions taken against organisations in 2010, we only have to look at the increase in personal data security breach notifications over the past year. Higher levels of awareness and stricter requirements under the Security Breach Code of Practice that we issued in July will have contributed to the increase. But this does not explain or excuse a tripling of the number of breach reports to our Office over the past year. It is clear that some organisations are failing to demonstrate accountability in regard to the personal data entrusted to them. This concept of accountability is important, and is dealt with later in the report. Notification of security breach incidents to our Office is not an end in itself. Organisations should learn from each incident, should avoid repeating the same mistakes and should be alerted to broader weaknesses. For now breach notification is a voluntary process, but legal requirements in this area are already growing stricter. A mandatory regime in relation to organisations providing publicly available electronic communication services will come into effect in May 2011. Data controllers should use the intervening period to get their house in order.

Customer Service

In 2010 the Office continued to respond to large numbers of phone calls, emails and written communications from members of the public and organisations using personal data on a broad range of issues, from access rights to registration obligations. We continued our commitment to ensuring that every member of our team spends at least one day a month responding to queries on our helpdesk. We began this practice in late 2006. It ensures that all members of staff, no matter how specialised, remain aware and focussed on how their work impacts on the organisations and members of

the public that we serve. Everyone benefits from the broader knowledge and interaction gained when dealing directly with queries from our customers. Feedback from the helpdesk contributes directly to the development of guidance material for our customers and to the targeting of our audit function towards particular sectors where our customers have highlighted issues. Feedback from the helpdesk also helps to inform and to direct our outreach activities.

Our website, www.dataprotection.ie, remains the key information resource for our customers. It is regularly updated to ensure it remains relevant and accurate and that it addresses the main issues of concern to our customers.

We also try to remain as accessible as possible to members of the public and to organisations processing personal data. In the last 12 months, members of our team have given 52 presentations to various organisations, details of which are available in Appendix 2 – Presentations and Talks - of this report. Though we try to accept as many invitations to provide presentations as possible, unfortunately we don't have the resources to respond positively to every request. However, learning aids and presentations on various aspects of data protection are available on our website to help organisations if we cannot manage to attend a particular event. There has also been a welcome increase in the availability of specialised data protection courses.

We also continue to place great value on our interaction with the media as this provides a valuable platform for raising awareness among the public of data protection issues. We try to respond positively to interview requests and queries so that we can provide useful and timely advice for our customers in response to emerging issues. Queries from the media continued at the same level as in previous years.

Our new Irish Language Scheme under the Official Languages Act 2003 was approved in 2010 and will be in effect until 2013. We will continue to develop the services provided to our customers in both Irish and English, including by providing comprehensive information on our Irish language website, www.cosantasonrai.ie.

Governance

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

The Office utilises core systems and services provided by the Department of Justice & 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

In total my Office opened 783 formal complaints for investigation in 2010. This compares with 914 complaints in 2009. As highlighted in last year's report, this decrease can be attributed, at least in part, to a greater focus on our part on only conducting formal investigations where there is evidence of a likely breach of the law. Many other complaints are dealt with by providing the complainant with appropriate information on their rights.

The steady decline in the number of complaints under the Privacy in Electronic Communications Regulations (S.I. 535 of 2003 as amended) continued over the past year. In 2010 we opened a total of 231 complaints in this category including unsolicited direct marketing text messages, phone calls, fax messages and emails. This compares with 262 such complaints in 2009, 321 in 2008 and 538 in 2007. As a result of prosecutions that we brought in 2008 against a number of companies operating in the premium rate text messaging sector, the level of valid complaints to my Office against such companies has fallen dramatically. The efforts made by companies in that sector to improve compliance with the law are welcome. The role which the Communications Regulator is now playing in this area is also greatly assisting in ensuring that the sector operates in a responsible manner.

Unfortunately in recent years we have seen an increase in the use of unsolicited text messages as a form of marketing by businesses across almost every sector of the

economy. The economic downturn appears to have exacerbated this problem. More and more businesses are using this medium to target former or current customers. Most of the 231 complaints about unsolicited electronic communications received by the Office in 2010 related to marketing text messages sent by Irish businesses of all sizes. During the course of our investigations we invariably find that the offending businesses are unaware of the law which applies to such communications. They have no awareness of the rules governing subscriber consent and the requirement to provide an opt-out mechanism in each marketing message. Several case studies are included in this Report to demonstrate our willingness to use our prosecution powers against businesses that break the law in this manner and fail to learn from their mistakes. These successful prosecutions, serve as a warning to all those tempted to break the law in this area.

As in previous years, the vast majority of complaints concluded in 2010 were resolved amicably without the need for a formal decision under Section 10 of the Acts or a prosecution under the Electronic Privacy Regulations. In 2010 a total of fourteen formal decisions were issued. Thirteen of these fully upheld the complaint and one partially upheld the complaint. A total of 812 investigations were concluded in 2010.

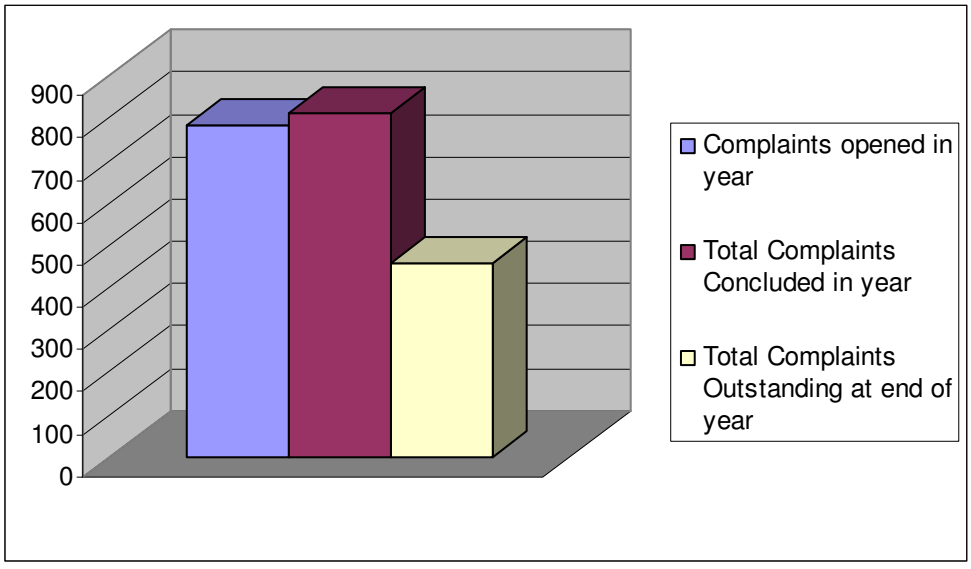


Figure 1- Complaints handling in 2010

Table 1 shows the breakdown of complaints by data protection issue. Excluding the 231 complaints concerning breaches of the Electronic Privacy Regulations, the remainder (70%) relate to breaches of the Data Protection Acts. The number of complaints regarding breaches of the Acts is down from 652 in 2009 to 552 in 2010.

Complaints concerning access rights accounted for 39% of the overall total. A total of 308 complaints about access rights were opened in 2010, compared with 259 in 2009, 312 in 2008 and 187 in 2007. This reflects strong public awareness of the right of access to personal data, a key fundamental right enshrined in data protection legislation. It likely also reflects the larger number of labour disputes arising from the redundancy of staff and the consequent need or desire of former employees to review how such decisions were made in their case.

	2010 Percentages
Access Rights	39.34%
Electronic Direct Marketing	29.50%
Disclosure	10.47%
Unfair obtaining of Data	1.92%
Failure to Secure Data	1.66%
Unfair processing of Data	10.22%
Accuracy	1.79%
Use of CCTV Footage	1.79%
Excessive Data Requested	0.64%
Postal Direct Marketing	1.79%
Unfair Retention of Data	0.38%
Other	0.50%
	100.00%

Table 1-Breakdown of complaints by data protection issue

Year	Complaints Received
2001	233
2002	189
2003	258
2004	385
2005	300
2006	658
2007	1037
2008	1031
2009	914
2010	783

Table 2 – Formal Complaints received since 2001

Use of Legal Powers

In line with previous practice in our Annual Reports, tables 3 and 4 below record a list of occasions when we were obliged to resort to the use of 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 in 2010 are set out in the following tables. While we may issue an

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

Data Controller:	In relation to:
Bus Éireann	Section 4 (1) of the Data Protection Acts
Roganstown Golf and Country Club	Sections 2(1)(c)(ii), 2A(1)(a) and 2D(1)(a) of the Data Protection Acts
RCabs	Sections 2(1)(c)(ii), 2A(1)(a) and 2D(1)(a) of the Data Protection Acts
Culfadda Housing Association Limited	Section 2(1)(a) and 2(1)(c)of the Data Protection Acts
Mulcahy Gorman Mulcahy	Section 4 (1) of the Data Protection Acts
P Harte & Co Limited	Section 4 (1) of the Data Protection Acts
P Harte & Co Limited	Section 4 (1) of the Data Protection Acts
Noxtad Limited	Section 4 (1) of the Data Protection Acts
Frank Heskin and Son Limited	Section 4 (1) of the Data Protection Acts

Table 3 - Enforcement Notices* issued in 2010

* 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.

Data Controller:
Ryan's Investments T/A Hertz Rent A Car
John Quirke & Co
The Lisheen Mine
Dunamagggin Credit Union Limited
Isaacs Group
Norfolkline Containers Limited
GMT Ireland Limited

Table 4 - Selected Information Notices* issued in 2010

* 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.

Data Breach Code and Group

The Data Protection Review Group established by the Minister for Justice, Equality and Law Reform reported in May. The Group had been asked 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. The recommendations of the Group were as follows:

1. Legislation should provide for a general offence by a data controller of deliberate or reckless acts or omissions in relation to the data protection principles – including contraventions of the security principle in relation to data breach incidents. This would complement the existing offence under the Data Protection Acts for failure to comply with an Enforcement Notice issued by the Data Protection Commissioner (DPC) - including an Enforcement Notice directing a data controller to inform individuals of a data breach affecting them.
2. The reporting obligations of data controllers in relation to data breaches should be set out in a statutory Code of Practice as provided for under the Data Protection Acts. The Code, broadly based on the current guidelines from the DPC, should set out the circumstances in which disclosure of data breaches is mandatory. Failure to comply with the disclosure obligations of the Code could lead to prosecution by the DPC.
3. The Code should be reviewed on a regular basis by the DPC and amendments submitted to the Minister as necessary to keep the legislation current.
4. The DPC should continue to develop his investigation and audit activities in a targeted way, with a particular focus on organisations which hold sensitive personal data, in compliance with emerging risk-based approaches to enforcement.
5. Legislation should provide for the timely publication of the outcome of such DPC audits, as an aid to good practice and in the interests of transparency.
6. The DPC should continue to develop public awareness activities in this area.

When publishing the Report, the Minister indicated that he would consider the recommendations of the Group in the light of anticipated changes in EU law on data protection. He asked that the Commissioner launch the process of preparing a Statutory Code of Practice, based on the existing guidelines, which would specify the circumstances in which the reporting of data security breaches to the Commissioner's Office would be mandatory.

A draft Code of Practice was published for public consultation at the beginning of June. The final version of the Code was published at the beginning of July, together with a Guidance Note. It was submitted at the same time to the Minister with a view to giving the Code statutory effect. This has not happened as of yet.

The key focus of the Code is on informing data subjects of a breach so that they can consider the consequences for each of them individually and take appropriate measures to protect themselves. It also requires reporting to our Office in most cases, the main exception being where the data has been made inaccessible in practice through use of strong encryption.

Data Breach Notifications

The introduction of the new Code of Practice had a marked effect on personal data security breach notifications to my Office. During 2010, my Office received 410 data security breach notifications from 123 different organisations. In 2009, we received 119 notifications from 86 organisations (see figures 2 and 3).

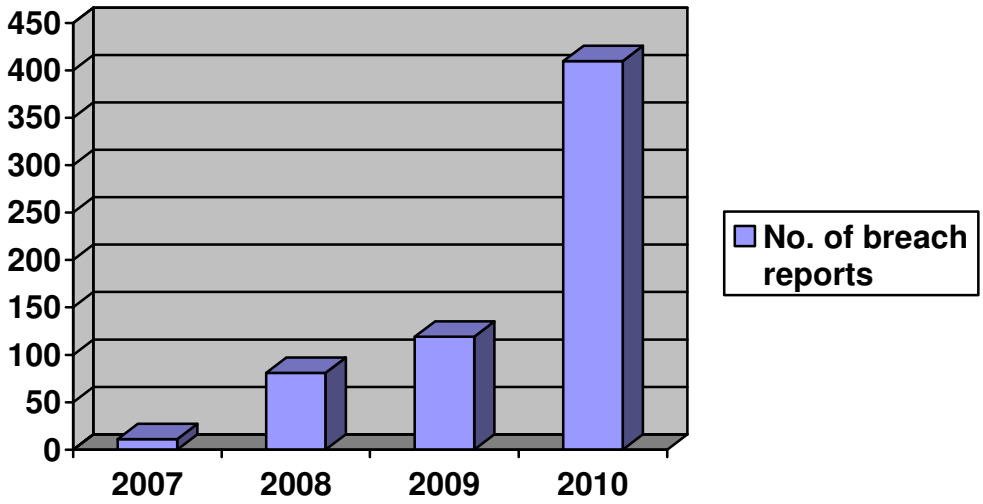


Figure 2 - No. of breach reports received annually

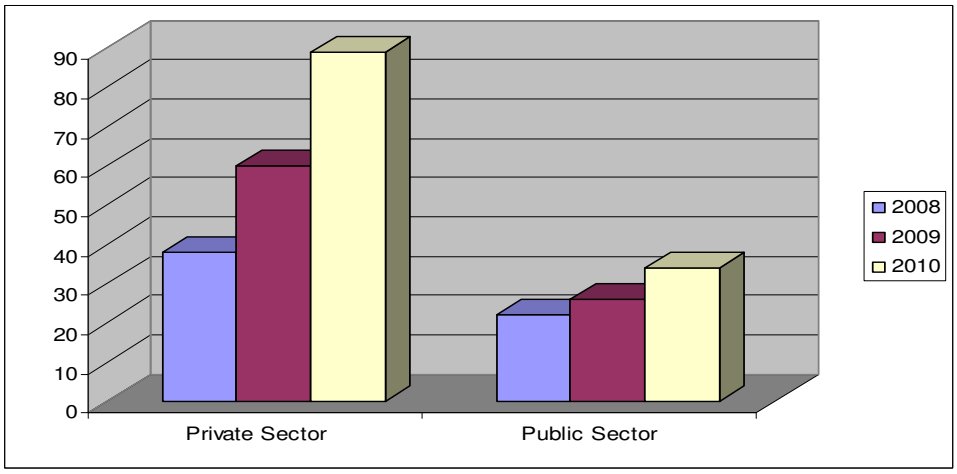


Figure 3 - Organisations reporting breaches by sector

However this increase of nearly 350% is not as alarming as it first appears. Until the introduction of the Code in July, the increase in the number of breach reports per month was more modest (see figure 4). It can be assumed that the sudden increase reflects the more exacting demands placed on organisations by the Code of Practice rather than an increase in the absolute number of data breaches. The Code demands particularly high standards of transparency from data controllers in the financial

sector and data controllers processing sensitive personal data, such as medical records. Over half of the reports received in 2010 came from these sectors.

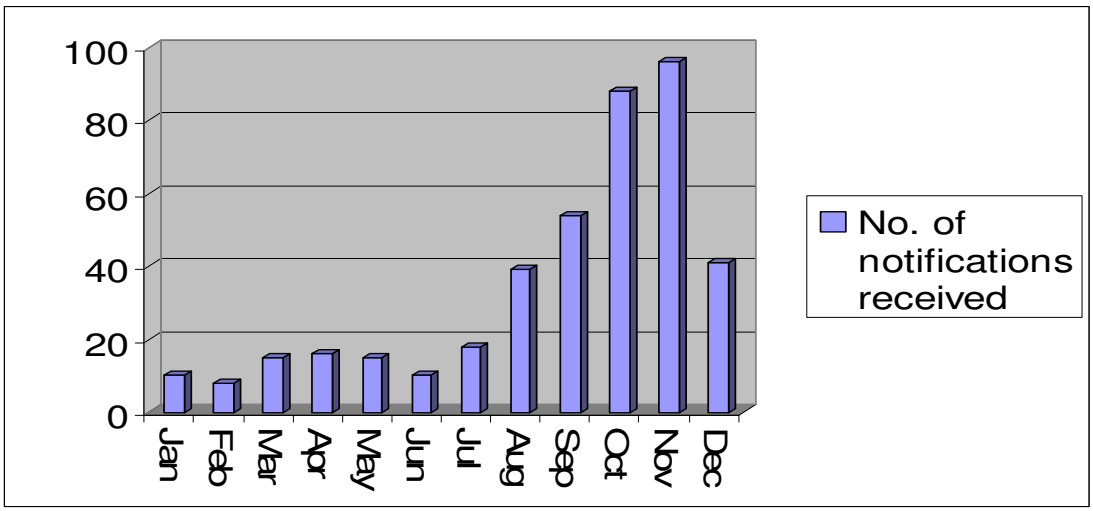


Figure 4 - Number of breach notifications received by month

The most common cause of data breaches reported is in relation to mailing, particularly traditional post as opposed to electronic mailing (see figure 5). There have been 258 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 the disclosure of which could cause distress or damage to affected individuals. Other noteworthy security breach incidents that took place in 2010 included the compromise of a GAA database, a hacking incident impacting on the website of SelfCatering.ie and unlawful access to Department of Social Protection records. More information on these incidents can be found among the case studies in Part 2 of this report.

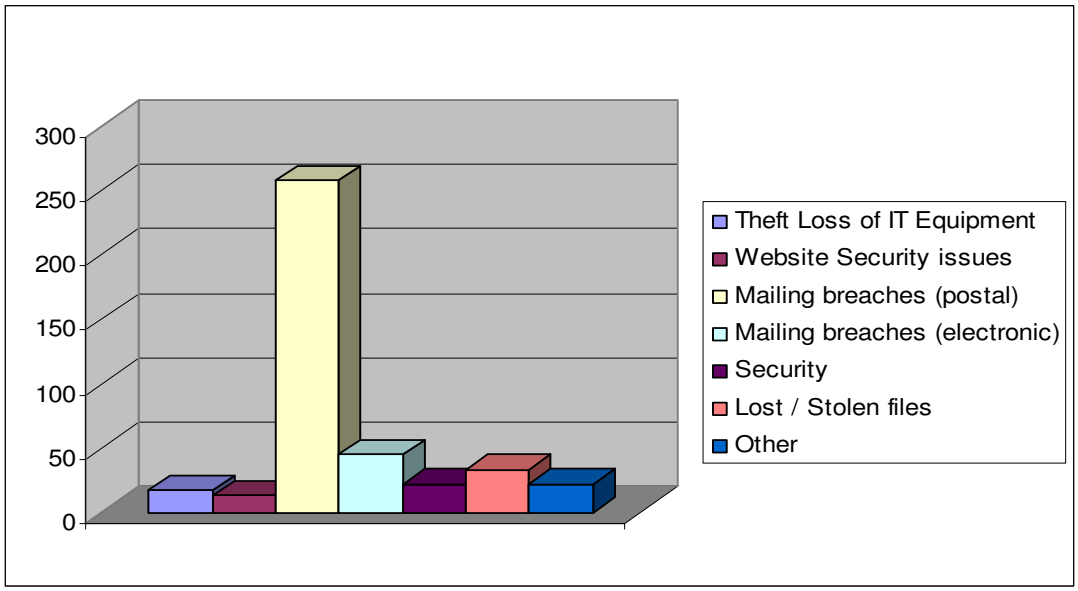


Figure 5 - Data security breach notifications by type

While the Code places increased demands on some organisations processing personal data and, indeed, on our Office, it has had a positive impact on levels of awareness of data security issues. It represents a strong incentive for data controllers to ensure that they design new systems with privacy in mind from the beginning, to continuously consider and address emerging risks to the personal data entrusted to them and to train their personnel to understand their obligations, so that breach notifications are minimised. Ultimately the tighter controls and greater transparency demanded by the Code will contribute to greater confidence among data subjects that their personal data will be managed in a responsible manner by public and private sector organisations. As the legal context in regard to mandatory data security breach notification changes across Europe, Irish organisations will be well-placed to adapt, thanks to their experience of the Code. As a recent study by the European Network and Information Security Agency (ENISA) noted:

> "stakeholders are looking for information and best practices from countries that already have notification procedures, either as a mandatory law or as a code of practice…both Germany and Ireland stand out as useful examples of countries that are already in the process of implementing data breach notification procedures."
> (ENISA "Data Breach Notifications in the EU" p.14-15).*

* http://www.enisa.europa.eu/act/it/dbn

Unlawful access to Department of Social Protection data

We received a breach report from the Department of Social Protection towards the end of the year which indicated that suspicions had arisen regarding an employee's access to social welfare records. Thanks to the Department's ability to audit staff access to its systems, an internal investigation revealed that records were accessed on a very large scale by the employee in question for no obvious reason. A link was also established to two specific phone numbers. As a result of this information, my Office was able to identify two private investigators of interest. Authorised officers visited the premises of the private investigator and in another case to their home having not gained entry at their registered premises which were closed. We obtained sufficient information from the visit to the premises of the first private investigator to establish the existence of business relationships, and provide for follow-up investigations with insurance companies. A subsequent visit to the auditors for the second private investigator allowed us to pursue financial institutions and debt collection companies who had an obvious relationship with the private investigator.

We are continuing an extensive investigation of this matter in 2011. We are focused on gathering sufficient evidence to bring criminal prosecutions, where appropriate, to send the strongest possible message that illegally accessing the personal information of citizens is not acceptable and carries serious penalties. We are also assisting the Garda Síochána (police) in relation to its investigations.

Privacy audits

We are empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Scheduled audits are intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive. They are sometimes supplementary to investigations carried out by the Office in response to specific complaints. Priorities and targets for audit are identified taking account of complaints and enquiries to the Office. During 2010 the Office continued to adopt a proactive role in this regard. In the course of the year, 32 comprehensive audits were carried out. The Office also continued with its

programme of unscheduled inspections under powers conferred under section 24 of the Data Protection Acts.

Organisations audited in 2010

The 32 audits carried out in 2010 represented an increase on the previous year, in which 30 audits were completed.

Many of the audits were focused on particular sectors, including the insurance sector, other financial institutions, schools, pharmacies and charities. We have observed new, potentially excessive, requirements for submission of personal data in all of these sectors.

Our inspection teams found that there was a reasonably high awareness of, and compliance with, data protection principles in the inspected organisations. However, the majority of organisations required immediate remedial action in particular areas. We noted with satisfaction that the majority of the audited data controllers have demonstrated a willingness to put procedures in place to ensure that they are meeting their data protection responsibilities in full. We are grateful to all of the organisations audited and inspected throughout the year for their cooperation.

List of Organisations audited

FBD Insurance
Bank of Ireland, Naas
First Ireland Insurance
Ulster Bank, Edenderry

Letting Agents:

- Caroline Bergin Property Management
- The Dublin Letting Company
- Dublinlettings.com

Lost Property Offices:

- Busáras
- Heuston

Dublin Bus

Dame Street Medical Centre
Permanent TSB, O'Connell Street
Paddy Power Plc
Concern
Risk Intelligence Ireland (provides services to insurance companies and others)
Cork University Hospital
RCabs (taxi firm)
Legionnaires of Christ
McCabe's Pharmacies
Commercial Mediation Services
Office of the Refugee Applications Commissioner
Reception & Integration Agency
The Refugee Appeals Tribunal
Asylum Accommodation Centre
Bus Éireann, Broadstone
St David's CBS, Artane
Dundalk Grammar School
Ard Scoil Rí
Boots Retail Ireland Ltd
Roganstown Town & Country Golf Club
J Rainey & Co. Ltd
Bailie Hotel

Department of Justice and Law Reform

In 2010, we commenced an audit of the asylum, immigration and citizenship process in the Department of Justice and Law Reform and of relevant agencies operating under the aegis of the Department. As the audit entailed the examination of substantial amounts of personal data across a number of agencies, the initial stages of the audit programme were focused on obtaining an overview of the asylum application and appeal process in terms of the capture and movement of personal data. Thereafter we conducted audits of the Office of the Refugee Applications Commissioner, the Reception & Integration Agency, an asylum accommodation

centre in the midlands and the Refugee Appeals Tribunal. The series of audits in this sector is continuing in 2011. It will entail audits of the Garda National Immigration Bureau and the Irish Naturalisation & Immigration Service.

Financial Institutions

In 2009 we received information from an employee in a branch of a large financial institution alleging that the branch was targeting marketing at customers, using their direct debit payment information to pinpoint areas for attention. On foot of this information, we made contact with the Irish Banking Federation and indicated our intention to conduct audits of branches in a number of financial institutions to investigate marketing practices at branch level. This was intended to give the sector an opportunity to amend practices to bring them into line with data protection obligations.

We also decided to use these audits as an opportunity to examine the procedures in place at branch level for:

- monitoring access to customer accounts;
- handling of requests from customers for changes of address or account holder information (e.g. joint account to single account);
- seeking information in the context of anti-money laundering requirements; and
- ensuring compliance with provisions in relation to the use of PPSNs (Personal Public Service Numbers) contained in the Return of Payments (Banks, Building Societies, Credit Unions and Savings Banks) Regulations 2008 (S.I. No. 136 of 2008).

Our findings were as follows

a) Marketing activities at branch level

In several financial institutions our investigations revealed marketing of customers on the basis of information contained in their direct debits, such as a monthly payment to another financial institution or a payment to the life branch of an insurance company. Direct debits are processed by financial institutions for customers as part of the banking services offered to account holders. The data contained within these transactions is not data to be used to target customers for marketing purposes. We

advise all financial institutions to ensure that there is no direct marketing activity within their organisations based on customer direct debit data.

b) Customer Accounts

One of Ireland's largest banks did not have the capacity to examine 'look ups' or 'views' by employees on its systems. This situation is unacceptable. We have instructed the organisation concerned to ensure the appropriate changes are made to their systems as soon as possible and we following this up.

At a sectoral level, we recommend that employee access should be reviewed on a proactive basis. Samples of logs should be checked at local level on a routine basis to detect any unusual access patterns. Once implemented, these new measures should be made known to staff to further discourage inappropriate access.

c) Anti-money laundering measures

In previous years we encountered a number of cases of over-reliance on anti-money laundering obligations to justify requests for personal data. We have received complaints from members of the public about the collection of excessive personal data, inappropriately justified as required to satisfy anti-money laundering obligations. In other cases, documentation provided legitimately for compliance purposes has been used for further, unacceptable purposes.

Anti-money laundering legislation does place obligations on financial institutions to seek certain documentation to establish the identity and to verify the current address of new customers. However, we are not convinced that this justifies the collection of further information at account-opening stage, such as income and employment details or details of the customer's main current account (including that other account's number and sort code). The collection of details such as the value of a person's home, the amount of mortgage outstanding, mortgage company, year of mortgage and mortgage type cannot be legitimised under AML requirements.

We accept that information regarding income may be sought legitimately in the context of an application for a credit facility. However, we cannot see the relevance of a person's income to the opening of a savings account unless the amount of a

lodgement gives cause for suspicion. We note that some financial institutions do not seek income details in relation to applications for deposit accounts, while other banks collect this information. In regard to employment details, such details may be relevant for anti-AML purposes for certain types of accounts but this does not justify collecting these details at account opening stage for every kind of account. In response to a complaint from a customer about the collection of excessive information at account opening stage, one financial institution stated that "information such as income, housing status, employment status, marital status etc. were used for tailored marketing and as information for future loan applications".

For the sake of transparency, we recommend that full details of additional data requested for anti-money laundering purposes should be outlined on all relevant account application forms/customer brochures.

Following the recent enactment of the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, we acknowledge that guidelines produced on foot of the transposition of the Third EU Anti-Money Laundering Directive into Irish domestic law will lead to the introduction of new standardised instructions on account monitoring. The passage of this legislation presents an opportunity to further clarify the boundaries of 'Know Your Customer' requirements and the extent to which these requirements justify the collection of customer personal data. It is however a disappointment that this very significant legislation, which sets aside data protection rights in a range of circumstances, was brought forward without any consultation with our Office. We did seek to provide, on our own initiative, some views at Committee Stage in the Oireachtas but this was too late to achieve meaningful change. There is significant tension between anti-money laundering and data protection requirements which create practical difficulties for organisations on the ground and the legislation presented a key opportunity to assist organisations and bring clarity in this area. This was missed. At EU level discussions are taking place as to the compatibility of provisions within the Third Anti-Money Laundering Directive with the Data Protection Directive which may require further changes to be made. Consultation with our Office may have afforded the State an opportunity to mitigate the need for further legislative changes on foot of the changes that can now be anticipated.

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 our Office.

Each year we receive a large number of requests for data protection training from organisations operating within the public, private and voluntary sectors. While we are not in a position to offer formal training as such, we seek to assist organisations within these sectors by giving presentations at appropriate events. During 2010, we made 52 presentations in total. We also have a large range of material on our website.[†]

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

Age-Targeted Awareness Raising

The findings from our most recent Public Awareness survey[‡] in 2008 indicated lower levels of awareness amongst the upper and lower age groups (65+ and 15-24 year olds).

In 2010, we continued to pursue an awareness campaign targeted at young people. In terms of the 12-18 year old cohort, we focused on the data protection resource produced by our 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). We were pleased to note the inclusion of a question on the CSPE 2010 Junior Cert Examination concerning Privacy and Social Networks which made direct reference to a piece on this issue featured in the CSPE resource booklet. This is indicative of the growing incorporation of privacy-related issues into the Irish educational curriculum. I am anxious to continue to promote the resource during 2011 and to engage with CSPE teachers via the Education Centres network. Data protection is also taught as part of

[†] http://dataprotection.ie/docs/Training_and_Public_Awareness/805.htm

[‡] Survey Key Findings (http://www.dataprotection.ie/documents/trainingandawarenes/PAS08.pdf)

Survey Full Report (http://www.dataprotection.ie/documents/press/Survey08.pdf)

the Leaving Certificate Business Studies course, highlighting the importance of data protection in a business context.

The National Centre for Technology in Education (NCTE) also continues to do valuable work in this area.

Policy issues

CCTV

The use of CCTV systems continues to give rise to regular complaints to our Office in a variety of contexts. On the positive side, I note that members of the public are beginning to question the widespread deployment and use of such systems. Many people are rightly concerned about the manner in which CCTV footage of them is used. It is encouraging that concerned members of the public are willing to challenge the data controllers in question and, if they are not satisfied with the response, to refer the matter to our Office. We should all recall that CCTV footage, while certainly having a useful purpose in a range of circumstances, is an intrusion into our personal space and therefore it is appropriate to question the justification for its installation in a range of circumstances. Particularly in the workplace and in schools, where employees and students can perhaps not feel able to voice their concerns, privacy rights are retained and there is a very high bar to justify any recourse to the use of CCTV systems.

In this context, we have targeted a number of schools for audit over the past year, usually in response to complaints. During such audits, schools must provide a convincing justification for the use of every camera in and around its premises. In addition, we examine control of access to monitors and footage. Where a school is unable to justify the use of particular cameras, they will be ordered to remove them. CCTV cameras are not a substitute for supervision and they should not be used for that purpose.

One of the many related cases that emerged in 2010 concerned the deployment of a CCTV system with cameras both outside and inside a primary school in Co. Mayo. In this case, the school installed the system without considering the issues it raised and

without developing policies to address those issues. Parents were justifiably concerned and representations were made to our Office on their behalf. Our investigation revealed that the requirements of the Data Protection Acts had not been met and we ordered the system to be switched off. In a separate case, a secondary school in Co. Kildare installed cameras in the student toilets. The students objected to this intrusiveness. When their concerns were dismissed, they walked out of the school in protest. As the cameras were operating in contravention of the Data Protection Acts, we ordered their immediate removal.

Complaints concerning CCTV in schools are not confined to students. On several occasions, school staff complained to our Office about the use of CCTV to review their movements. Under the Data Protection Acts, staff monitoring via CCTV is rarely proportionate. We have also encountered the use of web-linked CCTV systems to allow employers, based off-site, to monitor their staff carrying out their duties. This is highly intrusive and in most cases there is no legal basis for it under the Data Protection Acts. Where such practices have come to the attention of our Office, we have ordered that they cease immediately.

We have also included a case study in this report concerning the installation of a CCTV system by a housing association in a small village, Culfadda, in Co. Sligo. The Department of Justice and Law Reform has put in place a Community-Based CCTV Scheme and a Code of Practice for the deployment of community-based CCTV systems. The purpose of the Scheme is to support local communities who wish to install and maintain CCTV security systems to increase public safety and reduce anti-social and criminal behaviour in their area. The Scheme operates under Section 38 of the Garda Síochána Act 2005. The Code of Practice sets down strict conditions for the use of community-based CCTV systems in a manner that complies with data protection requirements. Outside of this Scheme housing associations and other community groups have no lawful basis for establishing CCTV systems for the purpose of policing their local areas or for any other purpose. Even where such systems are approved, it is the relevant local authority in that area that acts as the data controller with full responsibility, not well intentioned but potentially misguided groups of locals. We will require the removal of CCTV systems that have been set up for 'community-based' purposes outside of the Community-Based CCTV Scheme

established by the Department of Justice and Law Reform. Even for those schemes operating with approval, we have carried out a number of audits to ensure they are operating in compliance with the Acts.

Vetting Guidance

Over recent years our Office has received an increasing number of queries about vetting by the Garda Síochána for employment purposes. Given the varied nature of the queries, we compiled guidance about vetting to address the data protection considerations but also to provide general information about our understanding of the process in this jurisdiction.

Currently, the processing of personal data for vetting purposes is based solely on consent. We hope that this guidance note improves understanding of how information is processed when a person consents to be vetted for employment purposes. In addition, the guidance note highlights to employers the sensitive nature of the data which they may receive on foot of a vetting application and addresses the management of such data. Our Office recognises the necessity of vetting in relevant sectors and is satisfied that the model currently in use, as outlined in our guidance note, is compliant with the Data Protection Acts. However, if vetting is not done right, or in contravention of the guidance we have produced, it can have potentially very damaging implications for the individual and the process as a whole.

The guidance note can be accessed at the link below:
http://www.dataprotection.ie/docs/Guidance_Note_on_data_protection_considerations_when_vetting/1095.htm

Public Services Card

The Public Services Card which is scheduled to be launched in 2011 will be a key for public services in general and will, in time, replace cards that are currently in use, such as the Social Services Card and the Free Travel Card. Other Departments and agencies will also be in a position to use the card and its supporting infrastructure. The Public Services Card will include a photograph, signature and electronic chip, as well as featuring the PPSN of the individual on the back of the card.

We have flagged the phenomenon of function and information creep on a number of occasions over the past few years. We remain convinced, in light of experience elsewhere, that over-reliance on one form of identity creates weaknesses in security. Thankfully, we are not alone in our stance on this issue and Government policy at present is that the use of the PPSN must remain narrow.

We are concerned to ensure the card and the data stored on it are captured and processed in a proportionate and balanced manner. The incremental nature of the roll-out of the Public Services Card is welcome as is the active engagement of the Department of Social Protection with all stakeholders including our Office to try to ensure that all relevant issues are addressed. It has already completely taken on board a number of points which we have made, which I very much welcome. This incremental process allows the Department and organisations using the card to monitor its implementation and address any issues that may arise in advance of the card's universal distribution.

Data Sharing in the Public Sector

The issue of sharing personal data between state agencies, and the related issue of use of the PPSN, have featured regularly in our annual reports. The Data Protection Acts permit such sharing where the data subject concerned has given consent. Sharing is also permitted in a number of other circumstances set out in Sections 2A and 8 of the Acts. One such circumstance, set out in section 8(e), is when personal data is "required by or under any enactment or by a rule of law or order of a court".

Section 261 of the Social Welfare Consolidation Act 2005 is an example of legislation that permits sharing of personal data without consent. This provision is used extensively by the Department of Social Protection to seek information from other state agencies to assist it in ensuring that payments are only made to those eligible to receive welfare benefits.

In the course of the year, we engaged with the Department to ensure that its power to seek such data was only used in carefully defined circumstances, where the overriding of data subjects' right to control the use of their personal data was proportionate to the

objective of combating welfare fraud. The result was a set of Guidelines[§] published by the Department. The Guidelines can provide a basis for a general approach to data sharing within the public sector based on the principles set out below. Adherence to these principles should ensure that such data sharing is proportionate and in accordance with the Data Protection Acts.

1. Demonstrable Justification

The public policy objective being pursued by a particular data sharing arrangement without consent should be explicit. An assessment should be made as to whether the likely benefits of the sharing justify the overriding of the individual's data protection rights. The assessment should represent a careful balancing of these factors. It should take account of the fact that such sharing could increase the reluctance of individuals to provide accurate personal data to state authorities. It should also take account of any disproportionately negative impact on particular sections of society.

2. Explicit legal basis

The legal basis for data sharing, including the conditions under which such sharing is permitted, should be set out in primary legislation.

3. Authorisation

Any decision to share personal data between public bodies (and thereby to set aside a person's right to privacy) must not be taken lightly. This is especially the case when bulk data is shared. Such decisions should only be taken following due consideration at senior management level.

4. Transparency

If relevant, it should be made clear to individuals when they give personal data to a state body that this information may be shared with other state bodies. The reason for such sharing should be stated clearly. Under the Data Protection Acts, state bodies are legally required to include such disclosures in their public registration with our Office. In addition, it is good practice for a public body to regularly publish a list of their data sharing arrangements.

[§] http://www.welfare.ie/EN/Topics/Documents/DataMatchingSummaryGuidelines.pdf

5. Data minimisation

Only the minimum amount of personal data should be shared. In many cases all that is required is a "yes" or "no" in regard to whether an individual is, for example, a holder of a permit or a license.

6. Data access and security

Enhanced access and security requirements should apply to personal data received as part of an approved data sharing arrangement. Access to such data should be limited to a very small number of officials and security measures should rule out any possibility of data leakage (bearing in mind the increased emphasis on the State's responsibility to prevent data breaches and the reputational damage that would result from failure to protect shared personal data).

7. Data retention

Personal data provided as part of an approved data sharing arrangement should be securely destroyed when no longer required.

Given the concerns which we raised last year, it is important to formally acknowledge the constructive and pro-active approach adopted by the Department of Social Protection in the above engagements and more generally in relation to data protection matters. As referenced elsewhere in this report, the Department again demonstrated its pro-active approach in late 2010, when it discovered that an official appeared to be accessing customer data inappropriately. Such constructive approaches to data protection are also generally evident in the Office of the Revenue Commissioners and in many other large holders of personal data in the public sector, such as the Department of Foreign Affairs. This is very welcome and reflects the importance which these bodies attach to maintaining the trust of their customers.

We are also happy to report that An Garda Síochána continues to seek the guidance of our Office in meeting its data protection responsibilities. It is clear that the Gardaí are focused on maintaining high data protection standards when processing the sensitive data they hold. In 2007 we agreed a data protection Code of Practice with the Gardaí which included undertakings to monitor access to the Garda PULSE system. It is

disappointing to report that, despite our repeated engagements on this issue, the monitoring of access by members of An Garda Síochána to PULSE falls short of the standards we expect. We wish to see significant progress by the Gardaí in pro-actively monitoring PULSE access in 2011 and will be carrying out an audit to satisfy ourselves of this progress.

Charities and the collection of PPSNs

Section 848A of the Taxes Consolidation Act 1997 provides for a scheme of tax relief for eligible charities and other approved bodies in respect of donations received on or after 6 April 2001. This scheme is administered by the Office of the Revenue Commissioners.

Under the terms of the scheme, individual PAYE–only donors who make a donation to an approved body which qualifies for tax relief may complete a CHY2 Certificate and return it to the approved body. The approved body can then claim tax relief from Revenue as provided for in the legislation. The donor is required to record their Personal Public Service Number (PPSN) on this CHY2 Certificate. The PPSN is then recorded on the claim submitted by the approved body to Revenue for a refund of tax in accordance with section 848A.

In 2008 we became aware that charities were collecting and retaining PPSNs, purportedly for tax relief purposes, but in some cases retaining the details indefinitely on large donor databases. This practice came to light in the course of an audit of a charity. We instructed the charity to discontinue this practice and the situation was immediately rectified.

In 2009, we were contacted by members of the public about another charitable organisation that had pre-populated tax relief forms with the PPSNs of its donors. It then wrote to the donors enclosing the forms, seeking their signatures and confirmation of the donation amount. We subsequently audited this charity and discovered the same practice of recording PPSNs on a centralised donor database. In this case, the database contained the records of over 500,000 individuals.

We acknowledge that donors and volunteers are the lifeblood of all charities and are aware of the care that is taken by charities to manage and sustain these personal relationships. However, we were concerned to discover that the PPSN formed part of individual profiles on the donor databases maintained by some charitable organisations. It creates a risk of abuse of the PPSN and compromises the security of individual PPSNs. The retention or further use of the PPSN by charitable organisations is not justified. We have published guidance in 2011 advising all eligible charities and approved bodies that the retention of the PPSN is not in compliance with the Data Protection Acts. The guidance clarifies that it is a criminal offence under the provisions of the Social Welfare (Consolidation) Act 2005 to utilise and retain the PPSN outside of a narrow set of prescribed criteria. Charities do not qualify as specified bodies as set out in the Social Welfare (Consolidation) Act 2005. Therefore the sole legal basis under which they can process PPSNs is under Section 848A of the Taxes Consolidation Act 1997. The Revenue Commissioners have responded to our concerns by issuing a letter to charities with a new set of protocols in relation to the collection of the PPSN and the returns process in general.

We wish to thank the Office of the Revenue Commissioners for their assistance in this matter. We also received very constructive engagement from the Irish Charity Tax Reform Group on behalf of their members on the issue. They shared our view on this issue as they value above all the trust of their donors.

Archives

The Data Protection Acts (section 1 (3C)) provide that the normal restrictions on processing personal data (in particular the requirement that personal data should be securely destroyed when no longer required for the purpose for which it was first obtained) do not apply to:

(a) data kept solely for the purpose of historical research; or

(b) other data consisting of archives or departmental records (within the meaning of the National Archives Act 1986);

the keeping of which complies with such requirements as may be prescribed for the purpose of safeguarding the fundamental rights and freedoms of data subjects.

In 2008, we conducted a public consultation on draft regulations to address the proper balance between protecting personal data and facilitating research. Further consultation with interested parties – including the Director of the National Archives – took place in 2009 and 2010. In late September, a draft of the regulations was submitted to the Minister for Justice and Law Reform, whose consent is required to the making of such regulations.

The draft regulations attempt to balance the rights of individuals to control their personal data with the need for researchers to have access to such data. They are aimed at providing assurance to individuals that personal data relating to them retained for historical research purposes will be subject to appropriate privacy safeguards.

"Cloud" Computing

There has been much discussion in recent years of the model of "cloud" computing and its implications for the protection of personal data. While the concept means different things to different people, in essence it involves transfer of data to a data centre where the "cloud" provider processes the data. The extent of the processing can vary from simply housing the data to providing all of the facilities required to process it.

The key challenge for both the cloud provider and its customers is being able to guarantee the safety and security of the personal data in the "cloud". A report[**] by the EU body responsible for information security – ENISA – points to the paradox that holding data in the "cloud" can be both a risk and a protection: "…the cloud's economies of scale and flexibility are both a friend and a foe from a security point of view. The massive concentrations of resources and data present a more attractive target to attackers, but cloud-based defences can be more robust, scalable and cost-effective".

The ENISA Report summarises the challenge facing organisations considering outsourcing to the "cloud" (a challenge that is not limited to compliance with data protection law):

[**] http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

"Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g. between federated clouds. On the other hand, some cloud providers do provide information on their data handling practices. Some also offer certification summaries on their data processing and data security activities and the data controls they have in place, e.g. SAS70 certification."

It remains the responsibility of the organisation that chooses to outsource to the "cloud" to ensure that the data is safe. The well-established EU model of a data controller entrusting data to a data processor applies in many cases. Outsourcing requires not only a written contract but also active measures to ensure data is secure in the "cloud". If a cloud provider has taken the trouble to certify to recognised security standards such as ISO 27001 and SAS 70 or its successor SSAE 16[††], this provides significant reassurance about data security. But an organisation considering outsourcing also needs assurances about robust access controls, reliable data back-up systems and procedures in the event of data security breaches. Particularly where an organisation is subject to sectoral regulatory restrictions – financial services is a prime example – the organisation may not be satisfied to rely on third party certification and may want to carry out some form of audit at first hand. Finally, where the cloud provider is based outside of the European Economic Area (EEA), the rules on the export of data outside of the EEA must be observed.

Google WiFi and Street View Launch

Many large internet companies have their European headquarters in Ireland. Our Office continues to devote significant resources to assisting these companies to understand and comply with Irish and European data protection requirements.

In the case of Google, its Street View service was launched in Ireland at the end of September. We engaged intensively with the company in 2009 prior to the collection of images by its vehicles. We required it to publicly announce the collection of images and to provide updated information indicating the locations of the cars that

[††] http://sas70.com/sas70_faqs.html

were collecting the images. Google also agreed to devote resources to deal with any complaints both prior to and following the launch of the images. We received a relatively small number of complaints at the time of the launch and Google has taken steps to remove any image giving rise to privacy concerns. Google is continuing the process of image capture in different parts of the country, taking account of the general welcome given to the service by tourism and other interests.

Google also announced in May 2010 that it had inadvertently collected personal data as its cars collected the Street View images. Google described this as a technical engineering accident arising from the use of code to collect WiFi data that also collected "payload data" from routers. In some instances this included portions of emails etc in transit at the time the Google Street View car drove past. Google apologised unreservedly for the incident and undertook to put in place enhanced audit procedures. A number of investigations in relation to the incident were launched around the world. In Ireland, Google informed us of this incident in advance of the broader notification, due to the location of its European HQ in Dublin. We requested that it delete any payload data collected in Ireland immediately. We also requested that this should be verified by an independent third party. Google promptly complied with this request. We did not receive any complaints on this matter from the public though it did give rise to substantial media interest both here and abroad.

Engagements in the Education sector

The use of personal data in the education sector was a recurring theme throughout the year. We engaged with the Department of Education and Science, the Higher Education Authority, representatives of management bodies, the Irish Vocational Education Association (IVEA), the Vocational Education Committees (VECs), Institutes of Technology and teacher representatives. The key issue was finding a proper balance between the desire to collect personal data in relation to students for policy purposes and the data protection requirement that such data collection must be justifiable and have an appropriate legal basis. We have found a large amount of room for improvement in this area. We continue to engage with all the concerned parties to ensure that policy goals can be met while respecting the legitimate privacy expectations of students.

Cooperation with the Irish College of General Practitioners

During 2010, we were represented on a Working Group that included representatives of the Irish College of General Practitioners (ICGP) and the National General Practice Information Technology (GPIT) Project. The objective of the Working Group was to update a guidance document published by the ICGP and GPIT Group in November 2003 called "Managing and Protecting the Privacy of Personal Health Information in Irish General Practice – An information guide to Data Protection Acts for General Practitioners". Audits we carried out on a number of GP practices, which identified a large number of causes for concern, gave further impetus to the process of updating this document.

The revised document attempts to provide GPs with a straightforward and easy to use guide to data protection legislation while also addressing emerging issues to further assist GPs in meeting their obligations. It has been structured to support consideration of the data protection implications of the flow of personal information through a GP practice from the time it is first collected. The document reflects on the legal principles governing the use of personal data within a practice, when it can be released to third parties and how it should be stored and retained. Advice about patient access to their own information is also provided. A number of sample documents for use in GP Practices will also be appended. We hope that the finalised document will be published by mid 2011 by the ICGP, following a period of consultation.

Biometrics

We have expressed concerns in previous Annual Reports about the widening use of biometric data in our society and the potential effects of such processing. There is a risk that the general public will become desensitised by the roll out of biometric systems. We continue to receive complaints from the public about the deployment of such biometric systems. The most frequent complaints relate to the use of biometric time and attendance systems in the workplace and in schools. We have also received complaints about biometric systems recording customer attendance in commercial service providers such as fitness outlets. Substantial guidance material about the data protection implications of biometric systems has been published on our website. This

material gives clear advice to data controllers about the steps necessary to satisfy the requirements of data protection legislation before they deploy such a system. If they follow our guidance, data controllers are less likely to breach the Data Protection Acts. Regrettably, many data controllers install biometric systems without any consideration for the data protection rights of the people who they expect to use the system. This inevitably gives rise to complaints to our Office.

In regard to biometric systems in the workplace, our position on biometric time and attendance systems for employees was tested in the Circuit Court in 2010. During the course of a data protection audit of a major retail outlet, we found that a biometric system had been operating for some time. Staff had not been given an opportunity to opt out of using the system and they were not supplied with information about the processing of their personal data through use of the system. It was our view that the data controller was in breach of the Data Protection Acts. We served an Enforcement Notice requiring it to provide a range of information to its employees, including information on an alternative system for those who do not wish to use the biometric system. The data controller appealed the Enforcement Notice to the Circuit Court where the case was heard in full in April 2010. At the end of the hearing a settlement was reached when the data controller agreed to put up a notice at all of its hand-scanners as well as in its employee handbook and in its contracts of employment setting out a range of data protection information. It also gave an undertaking to the Court that if an employee objects to using the system, they will be informed of an alternative process. The alternative system would be considered by the data controller if a legitimate reason was put forward by the employee. The data controller accepted that this did not interfere with the Data Protection Commissioner's discretion to determine what might constitute a legitimate reason in any specific case. It was also confirmed to the Court that the Data Protection Commissioner would not regard a mere dislike of the system or desire not to use it as a legitimate reason which would give rise to an investigation on its part. We were satisfied with the outcome of this case. It supports the firm position that we have adopted with regard to the data protection rights of people who are asked to use biometric systems.

We are concerned that some employers wish to use biometric time and attendance systems as an alternative to the employment of staff supervisors, for night shifts in

particular. These employers appear to believe that, because a staff member must run their finger or hand over a scanning device on entering the workplace, there is some certainty that the staff are on-site and will remain there until the shift ends. This is taken to remove the requirement to employ a supervisor. This argument in favour of the use of biometric systems is not credible. While a staff member may turn up at their workplace and use the system to record their presence, the system does nothing to assure the employer that the staff member actually stayed on site or, even if they did so, that they performed their duties while there We will continue to adopt a very firm line in relation to the deployment of biometric systems in such circumstances.

Finally, during the course of an investigation concerning biometrics, we were interested to learn from a company which operates in the UK and in Ireland that opt-out rates differed significantly in each jurisdiction. In the UK, the company reported that only one percent of people opted out of using a biometric system to record customer attendance. In Ireland, the company experienced an opt-out rate of fifteen per cent. The opt-out rate which the company found in Ireland reflects our findings on the ground and, in particular, the level of calls to our helpdesk when organisations roll out biometric systems for the first time.

Roman Catholic Church audit exercise

We were contacted in early 2010 by the National Board for Safeguarding Children regarding data protection considerations associated with accessing personal data held by the Roman Catholic Church in Ireland. The National Board for Safeguarding Children was established by the Church bodies in 2006. Its remit is to advise its three sponsoring bodies (the Irish Bishops Conference, the Conference of Religious in Ireland and the Irish Missionary Union) on best practice relating to child protection policies and procedures. The Board also develops policies and procedures to guide the Church at a broader level about best practice in safeguarding children. Another function of the Board is to monitor, audit and review Church practices. It was in relation to this last function that the National Board sought the advice of our Office.

We were advised that an auditing exercise had commenced in line with the functions of the Board. However, shortly after the evaluation process began, data protection

issues were raised. As a result, the audit process was suspended pending clarification and assistance from our Office. We were asked to assist in finding a data protection compliant mechanism to allow the Board to assess the Church's current policies and practices on the safeguarding of children and to ensure that allegations of abuse were handled appropriately.

We welcomed the engagement. It facilitated successful navigation of the complex data protection issues that must be considered when examining the processing of sensitive personal data by a large number of separate, constituent organisations. These results were communicated in subsequent meetings with the sponsoring bodies of the National Board.

Limerick Regeneration Project

In the Annual Report for 2008 we outlined details of our engagement with the Limerick regeneration agencies and other statutory and voluntary agencies working in the Limerick area. The engagement related to sharing personal information on the provision of services to children and their families. Since then, and particularly during 2010, we continued to engage with the Health Service Executive (HSE) in the Limerick area (the HSE has responsibility for establishing information sharing protocols and early warning systems to address the needs of children). We welcome this ongoing commitment to developing processes in compliance with the Data Protection Acts. We have also benefited by gaining a more detailed understanding about the requirements of this sector in relation to the processing of personal data.

EU & International Responsibilities

Article 29 Working Party

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

The Working Party's activity in the course of 2010 had a significant focus on influencing the future EU data protection regime. Following its general opinion on the "Future of Privacy" published at the end of 2009, the Working Party produced specific opinions in the course of the year on the definitions of data controller and data processor, on the principle of accountability and on applicable law. The views of the Working Party found significant echo in the European Commission's Communication[‡‡] "A comprehensive approach on personal data protection in the European Union" published in November.

The Working Party also gave its views on: online behavioural advertising; aspects of international data transfers; RFID Applications; implementation of the Data Retention Directive; and a Code of Conduct for on-line direct marketing.

All of these documents are available on the Working Party's website.[§§]

During 2010 the Working Party continued to make progress in facilitating multinational companies to safely transfer personal data outside of the European Economic Area. The system of "Binding Corporate Rules" (BCRs) was further developed to better facilitate transfers of personal data to processors established in third countries. 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. For the first time we took on the role of lead authority in respect of one BCR application and reviewed a second application as part of a mutual recognition procedure entered into by a number of EU member states. This mutual recognition procedure is designed to streamline the BCR application process and make it easier for applicants to demonstrate compliance. We look forward to continued refinements in the BCR process to the benefit of all.

[‡‡] http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf
[§§] http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm

During 2010, the European Commission, based on advice from the Article 29 Working Party, formally decided that Andorra and the Faeroe Islands should be considered "adequate" for the free transfer of personal data from the EEA to these territories.

Third Pillar Groups

The Office continues to be represented at meetings of groups dealing with cooperation in the fight against crime. These groups include the EUROPOL Joint Supervisory Body (which reviews the activities of the European Police Office to make sure that its use of personal information does not violate individual privacy rights), the Customs Joint Supervisory Authority (which ensures that personal data within the European Customs Information System is processed in a manner that respects data protection rights) and the EUROJUST Joint Supervisory Body (which ensures that cross-border cooperation between EU judicial and prosecution authorities respects data protection rights).

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

- European Commission proposals and public consultations regarding a review of the European Union's data protection legal framework, including in relation to police and judicial cooperation, in response to changes brought about by rapid technological development and globalisation.

- European Commission proposals regarding the implementation of the Stockholm Programme (An Open and Secure Europe Serving and Protecting the Citizens) adopted by the European Council in December 2009. The Programme lays down priorities in the area of freedom, security and justice for a five year period.

- Data protection standards in the Terrorist Finance and Tracking Program (TFTP) II Agreement and other agreements designed to facilitate the exchange of personal data for the purpose of preventing, investigating, detecting or

prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters.

International Activities

We were represented at the Spring Conference of European Data Protection Authorities hosted by the Czech data protection authority and the 31st International Conference of Data Protection and Privacy Commissioners hosted by our colleagues in Israel.

We continued to follow the useful work being done in the OECD, especially in the area of cross-border enforcement of data protection. 2010 also marked the 30th anniversary of the adoption of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*** There were a number of events held throughout the year to mark this significant anniversary at which we participated and which also served to give a renewed focus to the applicability of the Guidelines.
We continued to assist our colleagues, in the EU and elsewhere, where they were dealing with complaints in relation to Irish-based organisations or seeking information on our data protection practices. We also contributed to "twinning" projects between the Spanish Data Protection Agency and the Data Protection Authorities of Croatia and Israel.

We continued to participate in the "accountability" project during 2010. The project is led by the US-based Centre for Information Policy Leadership. It explores what an organisation needs to do to demonstrate that it can be trusted to handle personal data responsibly. In 2010 the project moved into a second phase – facilitated by the French Data Protection Authority - focussed on how to demonstrate and measure accountability. A Discussion Paper††† on this topic was produced in October. The Article 29 Working Party produced a paper on accountability during the year that references the project.

*** http://www.oecd.org/document/20/0,3343,en_2649_34255_15589524_1_1_1_1,00.html
††† http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

The launch of what is known as the Global Privacy Enforcement Network (https://www.privacyenforcement.net/) was a welcome development in 2010. The initiative facilitates the sharing of privacy regulation experiences and best practices among privacy enforcement authorities from around the world. It is led by the US Federal Trade Commission. We were happy to be one of the founder members of this valuable initiative.

We participate as a Board Member on the European Board of the International Association of Privacy Professionals (IAPP)[‡‡‡]. This is a dramatically growing organisation that is providing a focus on the role of privacy officers and other privacy professionals in organisations. We also provide the chair of the Commission for the Control of INTERPOL's Files - the independent data protection oversight body of the International Criminal Police Organisation, INTERPOL.

Administration

Running Costs

The costs of running the Office in 2010 were as follows:

	2009 (€)	**2010 (€)**	**% change**
Overall running costs	1,814,553	1,449,329	20% decrease
Receipts	578,817	629,668	9% increase

Table 5 - Running costs

A fuller account of income and expenditure in 2010 is provided in Appendix 3.

[‡‡‡] https://www.privacyassociation.org/

Part 2

Case Studies

Case study 1: Ice Communications Ltd prosecuted for failure to comply with legal notices

In April 2009, we received a large number of complaints against Ice Broadband (also known as Ice Communications Ltd) concerning the disclosure of personal data as a result of an email issued by Ice Broadband. The email was entitled 'Disconnection Notice' and was sent to over three hundred customers. Among other things, the email stated that the customer's account was in arrears and that, unless contact was made within twenty four hours, their service may be cancelled and their account may be passed to its legal department. Ice Broadband included all of the email addresses openly in the 'To' field of the email, thereby disclosing the email addresses (and therein the identity of the recipients in many cases) and the content of the email to every customer to whom it was sent. Apart from complaining about the disclosure of their personal data, some customers expressed further annoyance that they had been sent the email at all since their accounts were not in arrears.

We began our investigation into this matter by immediately contacting Ice Broadband. We instructed the company to issue an email of apology to all affected customers. On receipt of our request, Ice Broadband immediately issued an email of apology to all those affected by the disclosure. My Office then sought a full report from Ice Broadband on the cause of the incident. We asked the company to outline the steps it had taken to ensure that such a disclosure would not recur. Approximately six weeks later we received an incident report from Ice Broadband in which it provided some detail on the cause of the incident and the steps taken to prevent a recurrence. However, the report contained some information which appeared to conflict with our understanding of the subject matter of the original email. As a result, we sought clarification on some aspects of the incident report. We also informed Ice Broadband of our obligation to attempt to amicably resolve complaints and we asked it to inform us of any proposals it wished to put forward to amicably resolve the complaints we had received. However, despite a number of reminders, Ice Broadband failed to respond to our letters. As a result, in October 2009 an Information Notice was served on Ice Broadband under Section 12 of the Data Protection Acts. It required Ice Broadband to provide certain information within twenty one days. We received an acknowledgement of receipt of the Notice from Ice Broadband's Customer Service

Manager. However, Ice Broadband failed to comply with the requirements of the Information Notice as it did not provide the information sought.

We received a separate complaint in July 2009 from one of the customers affected by the disclosure concerning a request she had made to Ice Broadband under Section 3 of the Acts. A Section 3 request obliges a data controller to inform the requester whether it holds any of their personal data and if so, to provide the requester with a description of that data and the purposes for which it is kept. The data controller must comply with the Section 3 request within twenty one days. In this case, Ice Broadband failed to respond to the Section 3 request. We commenced a separate investigation of this complaint. We wrote to Ice Broadband on the matter. However, it again failed to respond to our investigation despite three letters having been issued. Consequently, we served an Enforcement Notice on Ice Broadband under Section 10 of the Acts requiring it to comply with the Section 3 request within twenty one days. However, Ice Broadband failed to comply with the requirements of the Enforcement Notice.

As Ice Broadband had committed offences by failing to comply with the requirements of two separate legal notices served on it, we decided to prosecute the company. We served a summons on Ice Broadband to appear before the Dublin Metropolitan District Court on two charges. At the initial court hearing in March 2010, counsel for Ice Communications Ltd applied for an adjournment. He gave an undertaking to the court that the company would comply with the requirements of the Enforcement Notice and that it would provide the information sought in the Information Notice before the next court date. The court granted the adjournment and it fixed a hearing date for May 2010. On the same day as the initial court hearing, a liquidator was appointed to Ice Communications Ltd. At the end of April 2010, we received a letter from Ice Broadband in response to the information sought in the Information Notice. Around the same time, Ice Broadband wrote to the customer who had made the Section 3 request and it provided her with the information she had sought.

A full hearing took place in the Dublin Metropolitan District Court in May 2010. At the end of the hearing, the judge indicated that he believed that the company had committed a technical breach of the Acts and he found that the facts of the case

against Ice Broadband were proven. In his summing up remarks, the judge said that the company's managing director had buried her head in the sand in relation to the whole issue and he acknowledged that the Data Protection Commissioner 'had broken his back' in his efforts to obtain information from the company for the purposes of his investigations. In light of the fact that the company was now in liquidation, the judge indicated that he had to be realistic and impose a practical, common sense sentence. For that reason, he indicated that he would adjourn sentencing until the following day. He asked the managing director and the CEO of Ice Broadband to produce two personal cheques on the following day; one cheque was to cover our legal costs and a further cheque to the value of €1,000 was to be made payable to a charity of the court's choice. The cheques were handed to the court on the following day and the judge then applied the Probation Act in relation to the offences committed.

This case serves to demonstrate the lack of cooperation which we sometimes experience when investigating complaints. In truth, the investigation of these complaints should have been straightforward. A serious breach of the data protection rights of over three hundred people took place. The company should have responded with an immediate apology to the affected customers, an examination of the causes of the incident, an evaluation of the extent of the incident, remedial action to prevent such an incident from happening again and, finally, a full incident report to our Office. In this case, all of this could have been completed within 48 hours of the incident. Instead, the investigation was frustrated by the company to such an extent that we had to serve legal notices (which is something we do very sparingly) and, when the company failed to comply, we had to bring prosecutions. As a result, a matter which should have been dealt with over a couple of days following the incident took over a year to bring to a conclusion. The blame for that long process and the consequent consumption of our Office's resources lies solely with Ice Broadband. Had it engaged meaningfully with us on a cooperative basis at the outset, the issuing of two legal notices, one summons and the subsequent court proceedings could all have been avoided.

Case study 2: Free Spirit Hair & Beauty Salon Ltd / Crunch Fitness Limited / The Black Dog Communications Limited prosecuted for sending marketing text messages

We continued to use our powers of prosecution to ensure that consumers are not inundated with unsolicited marketing text messages to their mobile phones. A person's mobile phone is now almost an extension of the person and unwanted messages can be extremely intrusive. Regulation 13 of S.I. No. 535 of 2003 (as amended) provides that marketing text messages may not be sent to any individual unless that individual has consented to the receipt of such messages. Furthermore, it also prohibits the sending of marketing text messages without the inclusion of a cost-free opt-out facility which would enable the recipient to object to receiving further messages. It provides for penalties of up to €5,000 per message sent for each separate offence, or up to €250,000 on indictment or 10% of annual turnover if greater than this amount. A number of the cases that we prosecuted in 2010 are described below.

Free Spirit Hair & Beauty Salon Ltd

In 2009 we received two complaints concerning unsolicited direct marketing text messages promoting special offers from branches of Free Spirit Hair & Beauty Salon Ltd. One of the complainants had been a customer and the second complainant had made a treatment reservation which she later cancelled. Both individuals informed the Office that they had not consented to receiving marketing messages. Some of the marketing messages sent to these complainants did not contain an opt-out facility.

We contacted the branches concerned at the IFSC and at Citywest. Neither branch was able to provide evidence that the complainants had consented to receiving marketing text messages. On that basis we were satisfied that offences had been committed by both branches of Free Spirit Hair & Beauty Salon Ltd and we decided to prosecute those offences. This was not the first occasion on which this company had come to our attention. In 2006, during the course of our investigation of a separate complaint, we drew the company's attention to the law with regard to electronic marketing.

In January 2010, in the Dublin District Court, FS Citywest Limited and Free Spirit Hair and Beauty Salon Ltd pleaded guilty in respect of one offence each under

Regulation 13(1)(b) of S.I. No. 535 of 2003 (as amended) in respect of the sending of a direct marketing text message without consent. They also pleaded guilty to one offence each under Regulation 13(8) of S.I. No. 535 of 2003 (as amended) for not providing a valid opt-out address on those marketing messages. The Judge accepted the guilty pleas and imposed penalties of €250 for each offence. The Judge also ordered the defendants to pay our costs.

Crunch Fitness Limited

In 2008 we received a complaint regarding marketing text messages from Crunch Fitness Ltd. The complainant stated that she had no previous relationship with Crunch Fitness, that she had not given them her mobile phone number and that she had never consented to the receipt of marketing text messages from them. She informed us that she had contacted Crunch Fitness to find out how it had obtained her mobile phone number. She was told that the number had been collected in February 2008 when an individual had taken a tour of one of its gyms and had supplied the mobile number as a contact number. This was confirmed to us by Crunch Fitness. The company also confirmed that the individual who toured the gym was not the complainant. The text message also lacked a valid opt-out mechanism.

Crunch Fitness admitted that it had no opt-out facility in the message and indicated that, in future, an opt-out would be included in all direct marketing text messages. At this point, in May 2008, Crunch Fitness informed us that the complainant's mobile phone number had been removed from its marketing database. In line with our usual policy on such matters we noted their assurances and issued a warning.

The complainant contacted us again in December 2008 to inform us that she had received a further marketing text message from Crunch Fitness. Again, this message did not include any opt-out mechanism. In response, Crunch Fitness indicated that it had erroneously re-sent a message from March 2008. This resulted in the complainant receiving a further marketing message with no opt-out facility. On this basis we initiated prosecution proceedings.

In January 2010 the case came before Dublin Metropolitan District Court where Crunch Fitness Premier Limited pleaded guilty in respect of one offence under

Regulation 13(1)(b) of SI 535 of 2003 for the sending of a direct marketing text message without consent. The Judge accepted the guilty plea and imposed a fine of €500. The Judge also ordered the defendant to pay our costs. We have not had any subsequent valid complaints in relation to the company.

The Black Dog Communications Limited

In May 2009 we received a complaint from the mother of a thirteen year old girl who had received unsolicited marketing text messages from The Black Dog Communications Limited. As a result of clicking on a link in one of those unsolicited text messages, the child inadvertently joined a premium rate subscription service.

The complainant informed my Office that her daughter had previously entered a competition by text message in a teenage magazine. She assumed that this was the source of the premium rate subscription service. However, when she contacted the magazine, she was told that its competitions are stand-alone and did not involve joining a premium rate subscription service. She said that the magazine also assured her that information collected through its competitions is not disclosed to third parties.

When we investigated the complaint we found that The Black Dog Communications Limited had obtained the child's mobile phone number as a result of her entry to the competition in the magazine. This information gave rise to further questions as to how The Black Dog Communications Limited obtained customer information which was the property of a separate company. We subsequently established that both The Black Dog Communications Limited and the magazine used the technical platform of the same service provider to send and receive text messages for their respective services/competitions. A monthly report provided to The Black Dog Communications Limited by the service provider contained, in error, the mobile phone details of the entrants to the competition run by the magazine. The Black Dog Communications Limited placed those mobile phone numbers on its promotional database without checking to ensure that the numbers concerned had opted in to its database and without checking the basis for the consent.

We initiated prosecution proceedings and the case came before the Dublin Metropolitan District Court in February 2010. The Blackdog Communications

Limited entered a guilty plea in relation to one offence under Regulation 13(1)(b) of SI 535 of 2003 (as amended). Having heard the evidence, the Court was satisfied that the case against The Blackdog Communications Limited had been proven. Instead of recording a conviction and imposing a fine, the Judge applied the Probation Act on condition that The Blackdog Communications Limited make a donation of €3,000 to the GOAL charity for the Haiti Appeal and that it make a contribution to our prosecution costs. The Judge emphasised that the Court record would show that the facts relating to the offence were established and that that record would be available to the Court should the defendant come before it on any future occasion. We have not had any subsequent valid complaints in relation to the company.

Case study 3: Prosecution of Fairco Ltd / Pure Telecom for calling numbers listed on the NDD opt-out register

Making marketing calls to the line of a subscriber whose telephone number is recorded on the National Directory Database (NDD) opt-out register is an offence under Regulation 13(4)(b) of Statutory Instrument 535 of 2003 (as amended).

In April 2009 the marketing activities of Fairco Limited, a supplier of windows and doors, came to our attention when we received a complaint regarding a marketing call made by the company. The call was made to an individual who had exercised his right to have his preference not to be telephoned for marketing purposes recorded on the NDD.

By way of explanation, Fairco Limited informed us that while going through its database of past customers its operator dialled the wrong number and it apologised for its mistake. It provided us with details of the intended number. Unfortunately for Fairco, that number was also on the opt-out list of the NDD not to receive marketing telephone calls. In view of this we were not in a position to accept their explanation. In addition, this was the second time that this company had come to the attention of my Office. We initiated a prosecution in respect of the offence.

In March 2010, at Dublin Metropolitan District Court, Fairco Limited pleaded guilty in respect of one charge relating to the making of an unsolicited marketing telephone call to an individual without consent in April 2009 in contravention of Regulation 13(4)(b) of S.I. 535 of 2003 (as amended). The Court recorded a conviction, imposed a fine of €300 in relation to the offence and directed that our legal costs be paid.

Pure Telecom

During 2009 we received three complaints against a telecommunications company, Pure Telecom Ltd, regarding marketing calls made by the company to individuals who had exercised the right to have their preference not to be telephoned for marketing purposes recorded on the NDD opt-out register.

By way of explanation of two of these incidents, the company informed us that it had to reconfigure its firewall to allow access to new IP addresses following its move to new premises. The company stated that some of the older software had not been updated with the new addresses and therefore they were unable to connect correctly to the section of the database that held the most up to date NDD information. According to the company, for this reason these older systems were checking an out of date NDD list while the newer software was reading from the latest list (rhe NDD opt-out list is updated on a fortnightly basis and is circulated to marketers who are licensed to use it). This resulted in calls being made to numbers on the opt-out register. In another case, the company stated that it had obtained the phone number through a customer referral and that an off-shore telemarketing company working on its behalf had made the marketing call in that instance. The off-shore company had not checked the phone number against the NDD opt-out register resulting in a call for marketing purposes. We took the view that these explanations demonstrated procedural and system failures within Pure Telecom Ltd with regard to its telemarketing activities. We were satisfied that offences had been committed and decided to prosecute Pure Telecom Ltd in respect of those offences as, in line with our policy for prosecutions, the company had previously come to our attention

In May 2010, at Dublin Metropolitan District Court, Pure Telecom Ltd pleaded guilty in respect of three charges relating to the making of unsolicited marketing telephone calls to individuals without consent, in contravention of Regulation 13(4)(b) of S.I. 535 of 2003 (as amended). The Court recorded a conviction, imposed a total fine of €1,250 and directed that Pure Telecom Ltd pay our costs.

Case study 4: Tesco prosecuted for email marketing

In our Annual Report for 2008, we reported on complaints received from individuals regarding marketing emails from Tesco. In all cases, the complainants had registered for on-line shopping with Tesco and soon afterwards they began receiving marketing emails. Using the unsubscribe facility provided by Tesco, the complainants tried to stop further marketing emails being sent to them, but to no avail. Following our intervention, Tesco identified and fixed errors in its unsubscribe system. The complaints were resolved by means of an amicable resolution involving an apology and a goodwill gesture to each complainant.

In 2009 I was disappointed to learn that email marketing by Tesco emerged yet again as a source of complaint to our Office. We received a number of complaints from individuals who had attempted to unsubscribe from receiving further marketing emails. However, Tesco persisted in emailing them with promotional offers. One complainant reported that he had used the unsubscribe facility on the marketing emails several times and, when this did not yield results, he emailed Tesco's Customer Services requesting an opt-out. While several emails were exchanged between Customer Services and the complainant, Tesco continued to send marketing emails and we received a complaint. Another complainant experienced similar difficulties. He also attempted to unsubscribe using the facility provided on the marketing emails and, when these attempts failed, he sent an email to Customer Services reporting his efforts to unsubscribe. He informed Tesco that he was reporting the matter to our Office. Despite this, Tesco continued to send him marketing emails.

At the initial stage of our investigation we succeeded in having the email addresses of the complainants opted out of further marketing contact. It took some considerable time for Tesco to establish the cause of the failure to follow-up unsubscribe requests. Eventually, Tesco reported that the task of unsubscribing customers had been moved from Cardiff to India and that, following the move, the process had failed in some instances. In addition, Tesco reported that a separate problem arose when it introduced a new website platform. An error in the management of customer preference questions resulted in a failure to record those customers who had unsubscribed from email communication on the database.

On the basis of our investigation we were satisfied that offences under SI 535 of 2003 (as amended) had been committed. As this was the second occasion on which Tesco had come to our attention for breaching the instrument, we decided to prosecute. The matter came before the Dublin Metropolitan District Court in mid-2010. Tesco entered guilty pleas on four charges related to the sending of marketing emails to individuals who had requested not to receive such emails. The Court recorded a conviction on two charges and it took the other two charges into consideration. Penalties of €1,000 were imposed in respect of each of two charges. The Court awarded our legal costs to us. In addition, Tesco undertook to suspend all email marketing in Ireland until the errors in its opt out systems were corrected. One month later, Tesco reported to us that a solution had been found and implemented.

Unsolicited or spam email is one of the scourges of modern communications. It is something that affects all email users in their homes, at work or in their businesses. Most spam email comes from distant parts of the world, predominantly from outside of Ireland and the EU. Because of its origins, we do not have power to take action against the offenders. However, we investigate all complaints about unsolicited marketing emails sent by Irish based entities and, as this case study shows, we will not hesitate to use our powers to prosecute offenders if such action is warranted.

Case study 5: Individuals prosecuted for sending unsolicited marketing text messages

In addition to the other cases outlined in this report, we took prosecution proceedings against two individuals for sending unsolicited marketing text messages without including opt-out mechanisms in those messages. This was the first time that we pursued a prosecution in relation to an individual. The case has established an important precedent that Regulation 13 of SI 535 of 2003 (as amended) with regard to unsolicited communications applies not only to marketing companies but also to individuals, acting as data controllers, who are involved in marketing activity.

The Poker Room, operating from an address in Tallaght, first came to our attention in March 2008 when a member of the public lodged a complaint about persistent marketing text messages over a period of months. Despite replying to the text messages using the word 'stop,' he continued to receive marketing messages on his mobile phone. He informed the Office that he had no prior knowledge of this entity and that he had not supplied his phone number to it. During our investigation of the complaint we established the identity of the owner of the mobile phone number which was used to send the text messages. We wrote to that individual, informed him of the complaint, explained to him the law which applies to electronic marketing and sought his response. We received a reply soon afterwards indicating that the complainant's phone number had been removed from the marketing database and stating that the sender did not know that an opt-out facility was required in each text message. We then sent a formal warning to the individual that, in the event of any further complaints of this nature, we would consider a prosecution. We supplied a copy of our guidance material on electronic marketing. On receipt of that letter, the individual concerned phoned the Office to say that he was trying to make his marketing databases compliant. He undertook to include an opt-out mechanism in all future marketing text messages.

About six weeks later we were contacted by the same complainant to advise us that further text messages were being sent to his phone from The Poker Room. We also received a complaint from another member of the public indicating that he was receiving unwanted text messages from The Poker Club. He explained that he had

attended The Poker Club a few months previously and that he had given his phone number when signing up to participate in its games. He indicated that he had attempted to opt out by replying with the word 'stop' but this did not yield a result. He called in person to the venue where he asked at the reception desk that his phone number should be removed from the marketing list. After writing down his phone number and giving it to the gentleman working at the desk, he was informed that it would be taken off the mailing list immediately. Despite his efforts the text messages continued to arrive. He then lodged his complaint with us. At this point we had two valid complaints and we wrote to the same individual in relation to them. Our correspondence went unanswered. We then conducted a search on the Company Registration Office records from which we established that The Poker Room at The Square, Tallaght was a partnership business owned by two named individuals. One of the two business owners was the individual that previously engaged with us on foot of the first complaint. We wrote to the business at its registered address but we received no response to that correspondence.

We received a third complaint in 2009 from a doctor who was receiving unsolicited marketing text messages from The Poker Room in Tallaght and The Poker Room in Celbridge. She stated that she had not supplied her phone number to any such business. Similarly, the first complainant told us that he was now getting text messages advertising the Celbridge venue and that he had received a text message indicating that poker games at the Tallaght venue were being discontinued. During our investigations we found an internet posting by one of the business owners notifying the public that the Tallaght venue had closed and that all business had moved to Celbridge. We directed our investigations to the Celbridge venue and to the individual whose postings appeared on the internet. In a final effort, we wrote separately to the two business owners by registered post in January 2010. We received no response.

In light of the previous warning that we had issued in April 2008 regarding marketing text messages promoting The Poker Room and taking account of the fact that, despite extensive efforts on our part, The Poker Room and its business owners had failed to cooperate with our statutory investigation, we decided to prosecute the two business owners in their individual capacities. The defendants pleaded not guilty when the

case came before the Dublin Metropolitan District Court in July 2010 and a trial date was set. A full hearing took place in November 2010. The Court heard evidence from two of the complainants and from our Office. Both business owners gave evidence in their defence. One of the business owners told the Court that he had ceased to be involved in the business from around the middle of 2008 and he denied that he was responsible for the text messages which were the subject of the charges before the court. The Court accepted this and dismissed the charges against that individual. In relation to the case against the other individual, the Court ruled that the prosecution had proven its case in relation to ten of twelve charges. The Court recorded a conviction on one charge of sending an unsolicited marketing text message in contravention of Regulation 13(1)(b) of S.I. 535 of 2003 (as amended) and it imposed a fine of €1,000. The Court also recorded a conviction on one charge of sending a marketing text message without a valid address to which the recipient might send an opt-out request in contravention of Regulation 13(8) and it imposed a fine of €1,000. The court stated that all remaining eight charges were taken into consideration. The defendant was also ordered to make a contribution of €4,000 to our legal costs.

We were satisfied with the outcome of this case. Despite the failure of the business owners concerned to cooperate with our investigations, we persevered and ultimately brought them to justice in relation to the offences that had been committed. We afforded The Poker Room a chance to bring its marketing activities into compliance in 2008. Unfortunately it chose to take what appeared to be the easy option and to do nothing about its marketing database and procedures. The decision to ignore our warning in 2008 of future prosecutions cost one of its owners dearly in terms of penalties, legal costs and most of all, a criminal record.

Case study 6: UPC prosecuted for offences related to unsolicited marketing phone calls

In our 2008 Annual Report, we commented on the volume of complaints which had been received against UPC - then known as Chorus NTL. We had conducted a broad-based inspection of UPC on foot of the high level of complaints received. We issued a number of recommendations to the company as part of an audit report. We noted that the company had then taken a number of steps to improve its data protection compliance. However, we pointed out that there was no room for complacency and signalled that we would pay close attention to any further complaints against UPC to ensure that there was no slippage in terms of compliance.

I am disappointed to report once again that UPC remained the subject of regular complaint in 2010, especially with regard to direct marketing. In particular, the company's telephone marketing activities have been brought to our attention several times since the 2008 Annual Report. Following the investigation of a complaint received in October 2008 concerning a marketing telephone call, we warned UPC that any further such infringements would give rise to a prosecution. Despite the warning, further complaints were received. Following the investigation of two of them, we commenced prosecution proceedings against UPC in the Dublin Metropolitan District Court.

In 2009 we received a complaint from a UPC customer regarding a marketing telephone call that he had received on 1 July 2009 from UPC in relation to broadband services. The complainant supplied us with a copy of an email that he had sent to UPC in April 2009 requesting that the company use his phone number for contact relating to his account only and not for sales calls. He also supplied a copy of a reply he received in May 2009 from UPC notifying him that the company had complied with his request and that his account had been flagged for exclusion from marketing calls. If a telephone subscriber has notified a marketer that he/she does not consent to the receipt of marketing calls on their line it is an offence under Regulation 13(4)(a) of SI No. 535 of 2003 (as amended) for the marketer to make any further such calls to that subscriber's line. UPC admitted that the marketing call had been made as stated by the complainant. UPC explained that, due to human error by a customer service

agent, the customer's details were not properly removed from the marketing database. On receiving an opt-out request, an agent must put an indicator on the system by ticking the relevant options. In this case, the agent selected an incorrect option and only removed the customer's address from postal marketing. The agent failed to remove the customer's account from telephone marketing and consequently it remained on the telephone marketing list. Following our investigation, we were satisfied that an offence had been committed and we decided to prosecute that offence.

In early September 2009 we received a complaint from a UPC customer who stated that he had received a marketing call from UPC on 27 August 2009 in regard to digital television and high speed broadband services. The UPC customer supplied a copy of an email which he had sent to UPC in April 2009 stating that he did not wish to be contacted for marketing purposes in the future. We investigated the complaint. UPC acknowledged that it made the marketing call on the date in question. We established that a staff member at UPC had not passed the customer's email regarding his marketing opt-out to the responsible UPC department. UPC stated that this was a once-off occurrence and that the individual staff member responsible had been reprimanded and retrained. We were satisfied following our investigation that an offence had been committed and I decided to prosecute that offence.

The cases came before the Dublin Metropolitan District Court on the same day in April 2010. The Court accepted UPC's guilty pleas to each offence. The Judge imposed a penalty of €500 for each of the two offences and directed that UPC pay our costs in respect of the prosecutions.

Case study 7: Use of statutory powers to secure compliance with an access request

In May 2009 we received a complaint from an individual concerning the alleged failure of his employer, Mulcahy Gorman Mulcahy Accountants (MGM), to comply in full with an access request he submitted in February 2009. In support of his complaint, the data subject provided copies of documents that contained his personal data and that appeared to have been generated on the computer system of MGM. These documents were not provided to him in response to his access request.

We commenced an investigation by writing to MGM informing it that we had received a complaint from one of its employees in relation to an alleged failure to comply with an access request. We received a reply from the solicitors for MGM who informed us that its client had furnished the data subject with his personal file. The letter sought clarification and guidance on the type of documentation sought by the data subject. We informed the solicitors for MGM of the type of information the data subject was requesting and we reminded them of the obligation to comply fully with the access request. Following protracted correspondence with the solicitors for MGM, we did not receive confirmation of full compliance with the access request. Therefore we issued a final warning letter to MGM's solicitors informing them that enforcement proceedings would commence if its client did not respond in full to the data subject's access request. Prior to commencing enforcement proceedings, we received some personal data relating to the data subject from the solicitors for MGM. However, having compared this data to the data previously supplied to us by the complainant, it appeared that all the personal data to which the data subject was entitled had still not been furnished to him. In order to progress the matter and to ensure compliance with the Acts, we provided the solicitors for MGM with a list of the documentation which had been provided to us by the data subject and we requested that it comply with the access request within one week. Despite our best efforts, MGM failed to provide the data subject with all of his personal data within that timeframe.

In view of this unsatisfactory situation and the failure of MGM to meet its statutory obligation to respond in full to the complainant's access request, we concluded that

MGM appeared to be paying insufficient attention to the data protection rights of the individual concerned. Accordingly, authorised officers, using the powers conferred on them by Section 24 of the Data Protection Acts, entered and inspected the premises of MGM for the purpose of obtaining information that was necessary for the investigation of this complaint. During the unannounced inspection they found all but three of the documents which had been identified by the data subject as missing from the response to his access request. In the course of the investigation the data subject had provided us with some documents which he had received from MGM as part of his access request. It appeared that parts of these documents had been redacted and the data subject believed that the redacted parts contained his personal data. The authorised officers examined these documents during the inspection at MGM and found that the redacted parts of these documents did contain the personal data of the data subject and should have been provided to him in unedited form as part of his access request. The documents in question were emails sent between senior managers in the company and contained personal data concerning the data subject. We also found a further six documents containing personal data relating to the data subject which had not been released under the access request, the existence of which were unknown to the data subject.

At the end of the inspection, MGM gave the authorised officers a verbal undertaking that copies of all of the documents would be forwarded to the data subject within the following days. Despite this undertaking and despite numerous communications between our Office and MGM, the documentation was not voluntarily supplied to the data subject. We therefore served an Enforcement Notice on MGM requiring it to supply the outstanding personal data to the data subject. The Enforcement Notice was complied with within days of being served.

The events leading to instructions to authorised officers to conduct an inspection of the premises of MGM suggested that the company had a limited understanding of its duties under data protection law. When an individual makes an access request to a data controller there is a statutory obligation on the data controller to provide that individual with all of his/her personal data, subject to limited exceptions. In this case MGM failed to provide the data subject with some of his personal data without providing him with any reason for this decision. Our approach to complaints, as

provided for under the Acts, is to try to reach an amicable resolution. However, as demonstrated in this case, if a data controller fails to cooperate fully with an investigation we will not hesitate to use our statutory powers.

Case study 8: Unlawful use of CCTV images of a customer

We received a complaint in October 2009 from a solicitor, acting on behalf of a data subject, against a commercial premises located in Co. Cork. The complaint concerned the alleged gross misuse of CCTV footage at the premises. The solicitors informed us that the commercial premises had no signage in place to inform the public of the presence of CCTV and of its purpose. The complaint also alleged that on 1 October 2009 the data subject visited the premises and purchased some items. The staff member on duty was known to the data subject who spent some time speaking with him. The member of staff received a letter from the company that runs the premises dated 5 October 2009. The letter concerned a number of work performance issues relating to 1 October, including the fact that the staff member had spent time chatting with the data subject. The letter stated that the manager of the premises had examined footage from the security cameras at the premises. The employee concerned gave a copy of the letter to the data subject. That letter was passed on to my Office with the complaint.

Recognisable images captured by CCTV systems are personal data. Therefore they are subject to the provisions of the Data Protection Acts 1988 & 2003. To satisfy the fair obtaining principle of the Data Protection Acts with regard to the use of CCTV cameras, those people whose images are captured on camera must be informed about the identity of the data controller and the purpose(s) of processing the data. This can be achieved by placing easily-read signs in prominent positions. A data controller needs to be able to justify obtaining and using personal data by means of a CCTV system.

The subject of our investigation of this complaint was the capture and subsequent processing of the data subject's image on CCTV without his knowledge or consent. In its initial response to our investigation, the company informed us that it uses CCTV cameras in its commercial premises for security purposes. It also confirmed that CCTV was operating in this particular store without being properly notified to those visiting the store. It informed us that it was undertaking a review of the signage used in all of its stores throughout the country. It also apologised for any distress or

inconvenience caused to the data subject by capturing his image on CCTV without having informed him by means of appropriate notices in the store.

The first breach of the Data Protection Acts occurred when the data subject's image was captured on a CCTV camera located in a commercial premises that did not have appropriate signage in place. The second breach occurred when the company processed the data subject's image for a non-security matter (i.e. to address a work performance issue). We pointed out to the company that, regardless of whether there was signage in the shop to inform members of the public that CCTV cameras were in operation and their purpose, the processing of the data subject's image for a non-security matter was a breach of the Acts.

The Acts provide that, in the first instance, we must try to arrange an amicable resolution to a matter that is the subject of a complaint. The company agreed to seek an amicable resolution of the complaint. To that end it proposed to offer the data subject a letter of apology and a monetary goodwill gesture. The solicitor for the data subject subsequently confirmed his client's acceptance of the amicable resolution proposed. The company's letter of apology included confirmation to the data subject that his personal data had been erased and that the store in question now had a clearly displayed notice that CCTV was in operation.

Substantial guidance is available on our website in relation to the use of CCTV in a business or workplace. We encourage all data controllers, particularly those who may already have such recording systems in place, to familiarise themselves with this guidance.

Case study 9: Housing association install CCTV cameras in Culfadda

In November 2009, we received a complaint concerning the operation of CCTV by a local housing association in a small village, Culfadda in the west of Ireland. The complainant informed us that there were three CCTV cameras in operation in the village, one of which was located in the vicinity of a housing development for the elderly and the other two at private dwellings. The complainant alleged that all three cameras were monitoring public areas of the village.

We contacted the housing association and informed it of its obligations under the Acts in respect of CCTV usage. Recognisable images captured by CCTV cameras constitute personal data and, as such, are subject to the provisions of the Data Protection Acts, 1988 and 2003. Any data controller who uses CCTV needs to be able to justify obtaining and using personal data by means of the CCTV system. We provided the housing association with a copy of our guidance material on the use of CCTV. We asked it to outline how the processing of the images obtained from the CCTV cameras complied with the Acts and to give details of any signage that was in place informing individuals that CCTV was in operation. In response we were informed that the purpose of the cameras was to provide security for both the housing development for the elderly and for the village. The housing association asserted that the cameras only monitored public areas of the village and we were provided with more specific details about the operation of the CCTV system. According to the housing association, while the CCTV cameras had been installed, they were not yet operational. However, once planning permission for the poles had been approved by the local authority it was intended that the cameras would become operational. The housing association also stated that the housing development for the elderly was built by the housing association and was managed by it. We informed the housing association that, provided it was in compliance with the requirements of the Acts in relation to the operation of CCTV at the housing development for the elderly for which it had management responsibility, it could operate the CCTV system in respect of the exterior of those houses for security purposes. However, all other CCTV cameras recording footage from areas of Culfadda which were not part of the housing development for the elderly could not be operated by the housing association. The

housing association was also informed that, in the event that it obtained planning permission for the erection of the cameras in the village, this would not legitimise use of the CCTV system from a data protection perspective.

To ensure compliance with the Acts, we served an Enforcement Notice on the housing association. This is a legal notice requiring the housing association to cease or not to commence operating a CCTV system in the general areas of the village. It also required the housing association to comply with the provisions of the Data Protection Acts, 1988 and 2003, in respect of the operation of the CCTV cameras in the vicinity of the housing development for the elderly. We subsequently received an assurance from the legal representatives of the housing association that it would comply with the requirements of the Enforcement Notice. They informed us that the housing association proposed to apply in due course to the Department of Justice & Law Reform to operate the CCTV under the Code of Practice for Community Based CCTV Systems scheme provided for in the Garda Act 2005. It would be surprising if such approval was granted to a small village with relatively little history of crime; to do so would raise serious questions as to the proportionality of the measure.

Case study 10: Use of CCTV & biometrics at Boran Plastic Packaging Ltd

In late 2009, we received a number of separate complaints from employees of Boran Plastic Packaging Ltd located at Millennium Park, Naas. These complaints concerned the alleged use by management of CCTV on the factory floor for the purpose of monitoring staff and the use of a biometric system for recording employees' time and attendance. As both CCTV and biometric systems process personal data, their use is governed by the Data Protection Acts. We decided that the most effective course of investigation was to carry out an unannounced inspection at the premises in question to establish the facts.

In November 2009 two authorised officers carried out an unannounced inspection. While we use such powers sparingly, this is a useful means of establishing compliance with the Data Protection Acts. In general, authorised officers are treated courteously and receive full cooperation in the course of such inspections. Unfortunately that was not the case on this occasion. From the outset of the inspection the factory manager made every effort to frustrate the work of the authorised officers. It was made clear to them that their presence on the site was not welcome. Such was the level of discourtesy displayed towards the authorised officers in the performance of their functions that they considered issuing a caution against the factory manager with a view to formally charging him with obstruction - a criminal offence under Section 24 of the Data Protection Acts. However, the level of cooperation increased as the inspection continued. During the inspection Boran Plastic Packaging Limited denied that one of the purposes of the CCTV was to monitor staff. The company informed us that the main purpose of the CCTV system related to security and health and safety. On inspection of the factory, my authorised officers noted the location of the CCTV cameras. Based on information provided during the inspection, they noted that the individual who had access to monitor the CCTV images was a non-staff member. The individual in question was a member of the owner’s family and had off-site access to real-time CCTV views. It was also clear from our inspection that the company had no data protection policies in place in relation to the use of CCTV and biometrics. Following the inspection, the investigation progressed in the normal manner.

In our subsequent communications with the company we found Boran Plastic Packaging Ltd to be cooperative with our investigation. As a result of our extensive engagements with the company in the following weeks, it drew up a comprehensive data protection policy document. This document includes, among other things, its policy on the use of CCTV and biometrics in the workplace. The company's CCTV policy includes confirmation that there will be no live monitoring of images captured on CCTV and that recorded images will be viewed only following the rare occasions when an a security breach, employee personal protection or health and safety incident occurs. In relation to our concerns about access to the CCTV system, the company confirmed that access had now been restricted to two members of staff who had on-site access only. At our instruction, its policy on the use of the biometric system includes the provision that, should an employee have a legitimate privacy concern or any other concern in relation to the biometric hand scanner, they can contact a specific member of staff in the HR Department about their concerns. My Office informed the company that, if a legitimate privacy concern about the use of the biometric system is expressed by any employee to the HR Department, that employee has a right to opt out of using the system. We made it clear the onus is on the company to offer such an employee an alternative means of recording time and attendance. We informed Boran Plastic Packaging Ltd that, if it was to refuse such an employee the right to opt-out, he/she would have a right to make a complaint to our Office. Boran Plastic Packaging Ltd also confirmed that staff would be informed of the availability of a copy of its data protection policy documents.

The proliferation of CCTV and biometric systems in workplaces, without due regard to the data protection rights of employees and others, is a matter of great concern. Elsewhere in this Annual Report and in previous Annual Reports we have commented at length on these issues.

This case study also highlights the difficulties which my authorised officers face from time to time in carrying out their statutory functions. In most cases they receive cooperation from data controllers and their staff. We acknowledge that for a data controller or data processor an unannounced inspection can be a trying and anxious experience. However, for our part, we tend not to conduct such inspections unless we

have solid reasons based on complaints about breaches of the Data Protection Acts. Whatever the reason for the inspection, data controllers, data processors and their employees would be well-advised to cooperate fully with authorised officers. Authorised officers, in the exercise of their functions, have considerable powers conferred on them by law. Any obstruction or impediment placed in the way of the exercising of those powers is an offence and we will have no hesitation in prosecuting any individual, data controller or data processor who commits such an offence.

Case study 11: Lawful use of CCTV cameras by an employer

We received a complaint in September 2010 from solicitors acting on behalf of a data subject. The complaint stated that CCTV cameras were installed in the data subject's workplace without her knowledge and that the purpose of the cameras was to identify disciplinary issues relating to staff. The complaint also stated that CCTV evidence was obtained and used to dismiss the data subject for gross misconduct.

Recognisable images captured by CCTV systems are personal data. Therefore they are subject to the provisions of the Data Protection Acts. To satisfy the fair obtaining principle of the Data Protection Acts with regard to the use of CCTV cameras, those people whose images are captured on camera must be informed about the identity of the data controller and the purpose(s) of processing the data. This can be achieved by placing easily-read signs in prominent positions. A data controller must be able to justify obtaining and using personal data by means of a CCTV system.

With regard to the installation of covert CCTV cameras, our position is that the use of recording mechanisms to obtain data without an individual's knowledge is generally unlawful. Covert CCTV surveillance is normally only permitted on a case-by-case basis where the information is kept for the purposes of preventing, detecting or investigating offences, or apprehending or prosecuting offenders. This provision automatically implies an actual involvement of An Garda Síochána or an intention to involve An Garda Síochána. Covert surveillance must be focused and of short duration and only specific (and relevant) individuals/locations should be recorded. If no evidence is obtained within a reasonable period, the surveillance should cease.

If the surveillance is intended to prevent crime, overt cameras may be a more appropriate measure, and less invasive of individual privacy.

In this case we requested the data subject's solicitors to provide us with a copy of all correspondence that was exchanged in relation to the matter. On examining this correspondence, we noted that the data subject's employer considered it necessary to install the covert CCTV cameras because some members of staff informed the employer that money had gone missing from their purses. We also noted the

involvement of An Garda Síochána in the decision to install the covert cameras. We subsequently informed the data subject's solicitors that we did not consider that a basis arose in the Data Protection Acts to progress an investigation.

This case demonstrates the use of covert CCTV by a data controller in compliance with the Data Protection Acts. For personal data captured on covert CCTV to be fairly obtained and fairly processed under the Data Protection Acts, the installation of covert CCTV must involve An Garda Síochána or a clear intention to involve An Garda Síochána, as was the case in this instance.

Case study 12: Biometric systems deployed by commercial service providers and schools

During 2010 a customer of a large fitness chain contacted us. She reported that she attended the gym every day where she scanned a keyfob to record her attendance. Without any notice, the scan system was removed and she was told that in future she would be required to record her attendance using a new biometric system. She was asked to provide her fingerprint to facilitate use of the system. She was given no information about the processing of personal data involved in using the biometric system and she was given no opportunity to opt out. As a result of this and related reports from customers of the gym, we commenced a detailed and lengthy engagement with the fitness chain. It was clear that the organisation was not aware of the data protection issues arising from the use of its new biometric system until we made contact. It was also clear that frontline staff lacked the knowledge of data protection necessary to handle queries from concerned customers. We achieved a satisfactory outcome involving the removal of the mandatory requirement to use the biometric system and the provision of detailed information to customers about the processing of their data if they chose to use the system. For those customers who chose not to use the biometric system, a proximity card system was introduced. Consent is a critical consideration for the use of a biometric system. Customers should not normally be asked to use a biometric system unless they have given their consent and their consent must be informed; they must be given detailed information about the processing of their personal data before they decide whether to use the system. People must be told what their biometric data will be used for, who has access to it, what security measures are in place to protect it and how long it will be retained. They must receive assurances that their data will not be disclosed to third parties. Furthermore, those who choose to opt out must not be penalised. In this case the organisation attempted to impose a charge on customers who wanted a proximity card. We intervened to prevent this because a person may not be charged for exercising their legal right to opt out under the Data Protection Acts (we have no objection to the imposition of a small fee to cover the cost of supplying replacement cards to customers who lose or damage a proximity card).

In 2010 we continued to receive reports about the introduction of biometric systems in schools and other places of education to record student attendance. For example, it came to our attention that a large secondary school introduced such a system in January 2010. It announced the deployment of the system in a short note in its news bulletin. The notice was headed "Education (Welfare) Act, 2000" and stated that the provisions of that Act required it to promote school attendance. It went on to state that the board of management had invested in a biometric attendance system. No reference was made to data protection issues and there was nothing to suggest that students had any choice about using the system. Our guidance note on the use of biometric systems in educational institutions emphasises the requirements to obtain the signed consent of student users (and the consent of parents or guardians in the case of minors) and to give them a clear and unambiguous right to opt out of the system without penalty. When we contacted the school we were informed that attendance at the school implies acceptance by students and their parents of the school's policies and procedures. We responded that it was obvious that the informed consent of students and parents had not been obtained in line with our guidance and that, as a result, the continued use of the system was unlawful. We required the school to immediately seek the written consent of students and parents and to put an alternative system in place for those who do not consent or who subsequently withdraw consent. The matter was resolved to our satisfaction. I expect any educational establishment which has deployed a biometric system to keep a record of all written consents for as long as the relevant students are using the system. Authorised officers from my Office will examine the audit trail of consents in the event of an inspection.

Case study 13: Tracking Devices in Vehicles

During 2010 we received a number of complaints and general queries in relation to the deployment of tracking devices in vehicles such as cars and vans used for business purposes.

We received two separate complaints against a single company that installed tracking devices in company cars and in private cars used by their owners for business purposes connected with their employment. The complainants alleged that they felt they were being tracked and monitored 24 hours per day, 7 days per week as they had no means of switching off the tracking devices. The owner of the private car also expressed concern that his wife and children were being tracked when they were using the car outside of working hours. The user of the company car explained that he had use of the car for personal purposes outside of working hours and he complained that the tracking device created a huge intrusion into his private life.

In the course of our investigation of these complaints, we engaged at length with the company concerned and we met with them to discuss all of the data protection issues arising. We explained that the use of tracking systems in vehicles can give rise to data protection issues if they are not deployed in a manner that takes account of the legitimate privacy expectations of vehicle drivers, particularly when they are off-duty. Monitoring or tracking, including in-vehicle monitoring, must comply with the transparency requirements of the Data Protection Acts. Staff must be informed of the existence of the tracking equipment and of the purposes for which their personal data is processed. We established during the course of our investigation that, while privacy switches were fitted when the tracking devices were installed, the drivers were not shown how to use them.

The complaints were resolved to the satisfaction of the complainants and the company concerned on the basis of the following guidance from my Office. We expect any organisation deploying vehicle tracking devices to abide by these rules:

- If a company vehicle is permitted to be driven for personal use outside of working hours, a privacy switch must be fitted.

- If a privately owned vehicle is used for work purposes, a privacy switch must be fitted.
- The data controller is responsible for ensuring that drivers are given training on the operation of the privacy switch.
- The data controller must inform drivers of the purpose(s) for which the personal information processed by the tracking device will be used.
- The personal information processed by the tracking device may not be used for a purpose other than the stated purpose(s).
- Data controllers should devise and make available to drivers a policy on the use of tracking devices. This document should also set out the data controller's policy on the use of company vehicles for private use.
- New employees should be made aware of the existence of tracking devices on company vehicles and should be trained on the operation of the privacy switch.
- There is no requirement to fit a privacy switch if a company vehicle is used exclusively for work-related purposes, i.e. where no personal use of the vehicle is permitted.

Vehicle tracking devices are not staff tracking devices. Their key function is to track or monitor the location of the vehicles in which they are installed. Data controllers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff.

Case study 14: Hacking attack on SelfCatering.ie website

A bank made a data security breach notification to my Office in 2009 in relation to the credit cards of 1200 customers that had been compromised. SelfCatering.ie, an on-line holiday company, was identified as a common compromise point where all the cards had been used.

We contacted SelfCatering.ie and the Irish Payment Services Organisation (IPSO) to ascertain the full extent of the data security breach. It was determined that the timeframe during which the cards had been compromised was from May 2009 to June 2010. SelfCatering.ie informed us that an investigation had begun which involved a forensic examination of their computer systems. We requested a copy of the forensic examination report immediately on its completion. We also instructed SelfCatering.ie to cease processing personal data via its website until a reputable third party had certified that the website was secure for the processing of all personal data.

We obtained a copy of the forensic examination report for evaluation. It revealed that the website was not properly secured and had been subject to a SQL injection attack. The site did not comply with PCI (Payment Card Industry) security standards as required for handling on-line credit card transactions. The total number of credit cards that had been compromised was 9,500. The report revealed that 50,000 personal contact details held on the website may also have been compromised. It became evident during the course of my investigation that SelfCatering.ie believed that its hosting company was responsible for the security of its website. On that basis, the company had not ensured that the website was properly secured from external attacks through appropriate design and security measures.

We presented SelfCatering.ie with a list of issues to be addressed and a requirement for third party confirmation that these issues had been resolved, with particular emphasis on security measures. At our request, a prominent notice, the terms of which were agreed with our Office, was placed on the home page of the website to inform data subjects of the incident. This notice remained in place for 4 months. Those whose credit card details were affected were contacted directly by the relevant financial institutions.

This case was an example of a data controller using technology that it was unable to properly manage and obtaining personal data that it was unable to appropriately secure. My concern is that such problems are probably more widespread. Organisations intending to collect personal data on-line must take responsibility for ensuring that their websites are appropriately secure before accepting any on-line customers.

Case study 15: Compromise of a GAA database

In 2010 my Office investigated a data breach incident involving personal data of members of the Gaelic Athletic Association (GAA). In the course of the incident a database was compromised that contained the names and addresses of 500,000 members, the dates of birth of 289,000 members, mobile phone numbers for 107,000 members, landline numbers for 64,000 members and email addresses for 30,000 members (all numbers are approximate). In the case of 544 members, the database contained references to medical conditions. The database was hosted by Servasport Ltd., a service provider based in Northern Ireland contracted by the GAA for that purpose. Servasport confirmed that unauthorised access was gained to the database. At time of writing, this access is the subject of an ongoing criminal investigation by the Police Service of Northern Ireland (PSNI).

My Office received full co-operation from the GAA in the course of our investigation. The GAA informed all clubs of the incident and put in place a dedicated information line for any GAA members with concerns or who wished to establish whether their data was involved. The GAA wrote directly to any person whose health data was affected. As the incident has a cross-border element, we continue to liaise closely with our colleagues in the Information Commissioner's Office in Belfast as well as the PSNI.

The database in question was established to ensure a safe means of transmitting membership data. Unfortunately, in this case, it serves to illustrate the vulnerability of large centralised databases to inappropriate access. We sought to reassure those affected that there was no evidence that the data in question would be used for an illegal purpose or could be used to perpetrate identity theft on its own. However, affected GAA members should continue to be cautious in relation to any unsolicited contacts they receive through the post, over the phone or particularly via email that refer to their GAA membership and that seek to elicit further personal information.

Case study 16: Employee obtains data from customer file for his own use

In March 2010 we received a complaint regarding an alleged inappropriate access to customer personal information by an employee of Aviva (an insurance company). The complainant informed us that, in March 2010, he was telephoned by an individual who accused him of scratching his car on the previous evening while parking in University College Dublin. As the complainant knew nothing of this incident, he asked the caller how he had obtained his phone number. He was informed by the caller that he had noticed that the car was insured with Aviva and, as he worked for that company, he had sourced the phone number from the Aviva system. The caller stated that he had left a business card on the car windscreen. When the data subject checked, he found the business card with the name of the individual concerned and his job title.

We commenced our investigation of this complaint by writing to Aviva, drawing their attention to the obligation to keep personal data for specified, explicit and lawful purposes and use it only in ways compatible with these purposes. On this basis, we asked Aviva to outline the circumstances in which the complainant's personal data was processed in the manner outlined in his complaint. In its response Aviva assured us that it has very stringent procedures in place regarding the safeguarding of customers' personal data from unauthorised access and the protection of this data from processing for purposes other than for which it was collected. In relation to the specifics of this complaint, Aviva investigated the matter and raised it with the employee concerned. The employee confirmed that he accessed the policyholder's data for the purpose of contacting him to discuss the incident and to see if he wished to settle the matter directly with him. Aviva acknowledged that the incident should have been pursued in the normal manner through its claims procedure. If the correct procedure had been followed, the complainant's personal information would have been accessed by claims personnel and used to alert him of the allegation. Aviva informed us that the staff member in question had been made aware in no uncertain terms of the seriousness of the incident. In addition, the issues raised by this complaint was used to draw the attention of other staff members to the importance of complying with data protection obligations.

In an effort to amicably resolve this complaint, Aviva issued a letter to the complainant explaining what had occurred and apologising for the distress and inconvenience caused. The company also offered the complainant a voucher for €100 towards his next renewal premium. The complainant accepted this amicable resolution.

This complaint raised a serious data protection issue. Organisations are entrusted with a huge amount of personal data which they have a responsibility to keep safe and secure. The message that customer personal information can only be accessed on a "need to know" basis must be continually reinforced. While safeguards are required to protect customer data from disclosure to third parties outside the organisation, similar protection must be afforded to protect the data from internal misuse. This theme is raised again elsewhere in this report in relation to insurance companies. We must also acknowledge that we received full co-operation from Aviva in this matter and the company takes its data protection responsibilities seriously.

Case study 17: Inappropriate disclosure of medical research data

In March 2010 we were contacted by a lady who had received a telephone call from a university student asking if her husband would be interested in participating in a survey. The survey related to a disease suffered by her husband. As her husband was not at home at the time of the call, the lady suggested to the caller that she phone again at another time. On the following evening the lady answered the phone again to a different student about the same matter. On this occasion she questioned the caller about how he had obtained information about her husband's medical condition. She was informed that the student's lecturer had obtained the data from an affiliated hospital where her husband attended as a patient. She contacted our Office about her concerns in relation to the disclosure of her husband's sensitive medical information.

From the outset of our investigation we received full cooperation from the hospital and from the university. The incident was treated seriously by both entities and it was accepted by all sides that a breach of the Data Protection Acts had occurred.

Background

The hospital has a strong commitment to clinical research with a view to improving care for patients. This can involve collaboration with other institutions including colleagues in its affiliated university. Typically in this type of collaborative research, the research team from the University work closely with a multidisciplinary team in the hospital for the duration of the research proposal. This study had the full support of the clinical staff and every effort was made to facilitate recruitment of patients for the study. The normal procedure for clinical research is to recruit patients through advertising or during their normal clinic attendances. In this case, a decision was made to extract data from the hospital database and contact patients directly by telephone to arrange to meet them with a view to obtaining informed consent. This process change should have been brought to the attention of the relevant Ethics Committees. However, due to a misinterpretation of the approval and the researchers' obligations under the Data Protection Acts, the Ethics Committees were not informed.

The Breach

The breach of the Data Protection Acts took place when a qualified clinical researcher at the university was given printed copies of patient data from the hospital database

relating to the disease under research. After initial attempts to contact patients at scheduled clinics, a decision was taken by the clinical research team to contact the patients directly.

Action Taken Following Breach

On becoming aware of the breach the hospital immediately began an investigation. The patient recruitment process was halted and the data was returned. A review of the hospital's research ethics approval processes, data protection policies and communication procedures took place in the course of the investigation. It has established guidelines and policies for ethical approval of research proposals involving patients. The review prompted an update of the application procedure to include more detailed requirements for researchers in regard to recruitment, data collation and data protection issues. In future, the hospital will ensure that applicants are informed of their obligations and insist on attendance at appropriate good practice in clinical research courses. The hospital will also include a section dedicated to awareness of data protection issues in their regular workshops for researchers.

Following our investigation we are satisfied that a much greater focus will be applied to compliance with the Data Protection Acts in the course of such research projects. As the data controller in this instance, the hospital took full responsibility for the breach from the outset. It wrote to all of the affected patients to acknowledge the breach, to explain what had occurred and to apologise for it. The behaviour of the hospital in responding to this issue was impeccable and reassure me of its commitment to data protection and its determination to learn from this experience.

Case study 18: Unlawful disclosure of previous army career information

In September 2009 we received a complaint from a Civil Defence employee alleging that the Defence Forces had disclosed personal information regarding his previous army career in 1982 to a Civil Defence Officer in Co. Louth. The Civil Defence Officer allegedly circulated the information to other parties in a handwritten memo. The complainant supplied us with a copy of the handwritten memo which included comments relating to his army career. This memo was signed by the Civil Defence Officer.

There were two components to our investigation of this matter as it involved two separate data controllers and allegations of separate breaches of the Data Protection Acts against each of them. The breaches involved the alleged unlawful obtaining and processing by the Civil Defence Officer of information relating to the data subject and the alleged disclosure of the data subject's personal information to the Civil Defence Officer by the Defence Forces.

As Louth County Council is the data controller for personal data processed by Louth Civil Defence, we contacted it in relation to the allegation that one of its Civil Defence Officers unlawfully obtained the data subject's personal data. In our initial communication to Louth County Council, we requested that it clarify the purpose for which the Civil Defence Officer obtained the data subject's personal data from the Defence Forces and provide us with the name of the person in the Defence Forces who disclosed this information.

Louth County Council informed us that a Civil Defence Officer received an anonymous telephone call and, on foot of that call, he deemed it appropriate to make enquiries as to the data subject's previous record in the Defence Forces. We were told that the Civil Defence Officer, remarkably, could not recall the name of the senior officer of the Defences Forces who actually supplied the information. Louth County Council stated that the Civil Defence Officer subsequently received a return telephone call from another member of the Defence Forces (whose name he was equally unable

to recall) who supplied him with certain personal information relating to the data subject.

We contacted the Defence Forces on the basis of Louth County Council's response to our investigation. The Defence Forces informed us that it had conducted a search of the data subject's personnel file to check for any memo indicating that information had been disclosed to the Civil Defence Officer. We were informed that no such memo was found on the file. Without the name of the senior officer with whom the Civil Defence Officer communicated, the Defence Forces were not in a position to comment on the alleged disclosure.

To progress the investigation an authorised officer visited Defence Forces Headquarters to inspect the data subject's personnel file. On comparing the information on the data subject's personnel file with the information on the handwritten memo signed by the Civil Defence Officer, the authorised officer was satisfied that the information in the memo was sourced from the army personnel file. On this basis we concluded that the Defence Forces had breached Section 2 of the Acts by disclosing personal information without the data subject's knowledge or consent or other appropriate legal basis.

The Acts provide that our Office must try to reach an amicable resolution to a complaint in the first instance. The Defence Forces confirmed its interest in finding an amicable resolution. The data subject's complaint against the Defence Forces was amicably resolved when the Defence Forces issued a letter of apology to him. The Defence Forces expressed its regret for the release of his personal data in an unauthorised manner to a third party and it apologised unreservedly to him.

In relation to the complaint against Louth County Council, we were satisfied that Section 2 of the Acts was breached by the County Council when the Civil Defence Officer obtained and processed personal information relating to the data subject without his consent or knowledge. This complaint was amicably resolved when Louth County Council provided the data subject with a letter of apology in which it described the circumstances in which his information was obtained from the Defence Forces and acknowledged that the information should not have been sought or

obtained. The Council described how the information was subsequently divulged by the Civil Defence Officer to others. The letter assured the data subject that he had not suffered any disadvantage as a result of the Council being in possession of the information. The Council confirmed that the hand-written memo and any copies of it in the possession of Louth County Council would be shredded.

We view this case as a serious breach of the data protection rights of the individual concerned. We are concerned that a personnel file dating from 1982, which was in the control of the state, was retrieved and thoroughly searched for comments made by superiors. This information was then disclosed by phone to an outside party without any regard for the rights of the individual concerned.

Case study 19: Housing association discloses personal data to a debt collection agent

In June 2010, we received two separate complaints alleging that Léim an Bhradáin Housing Association, Leixlip, Co. Kildare inappropriately disclosed personal information. The complainants alleged that an individual, who was not an employee of the housing association, had personal information relating to them when he called in person to their homes. The information included contact details and an outline summary of their rent payments to the housing association. The complainants were concerned that their personal information had been disclosed to an individual who was unknown to them and who appeared to have no affiliation to the housing association.

From time to time organisations need to engage the services of an agent to process personal data on their behalf. Such an agent is termed a 'data processor' under the Data Protection Acts. When a data controller engages the services of a data processor, it must take certain steps to ensure that adequate standards of data protection are maintained by the data processor. A data controller is permitted to engage a data processor only on the basis of a written contract (or equivalent) which includes appropriate security and other data protection safeguards. Informal or ad-hoc arrangements do not meet the requirements of the law with regard to the processing of personal data by third parties.

On receipt of notification from our Office that we had commenced an investigation into this matter, the solicitors for the housing association responded that the association had engaged a third party to call to various tenants to request that they deal with the issue of rent review and bring any arrears of rent up to date. They stated that no information was furnished by their client to this third party. They also questioned the motivation of the complainants on the basis that they owed rent arrears and had done so for some time. They conceded that no written contract existed between the housing association and the third party. We responded seeking clarification of how the third party was in a position to visit certain houses on the estate concerning rent arrears without having been supplied in advance with the details of the people who were in arrears. The solicitor for the data controller responded claiming that we had prejudged the matter and our comments amounted to

an assertion made in advance of any determination in relation to the complaints. They requested that the investigator handling the case stand aside from the investigation and they threatened to issue proceedings against the Office if the investigation proceeded.

I cannot tolerate such behaviour as it amounts to an attempt to restrain the performance of my functions. We informed the solicitors that we would continue to perform our statutory functions in investigating the complaints and, in the absence of a response to questions posed as part of our investigation, we would use our legal powers to obtain the information required.

Following a further exchange of correspondence with the solicitors for Léim an Bhradáin Housing Association, the complaints were concluded. The data controller wrote to the complainants acknowledging the breach that occurred when they passed certain information to a third party. The housing association apologised for this and it assured the complainants that there would be no repeat of the incident.

The motivation behind the complaints was a recurring theme in the correspondence from the solicitors for the data controller, on the basis that both complainants were in substantial rent arrears. We only seek to establish if there is a legitimate data protection complaint; we cannot and do not question the motivation of complainants. We respect the right of data controllers to collect debts. However, the processing of personal data in the collection of debts must be carried out in compliance with the Data Protection Acts. The data protection rights of individuals cannot be disregarded simply because they are in debt.

Case study 20: Disclosure of management fees owed to a property management company

During 2010 we received several complaints in relation to the disclosure by property management companies (set up to manage housing estates) of details relating to individuals in arrears with payment of their management fees. In general these disclosures occurred through the circulation of a list of those in arrears to all members of the property management company. The list typically contained personal details such as house/apartment number, name and amount of arrears due. The general view of the property management companies was that an individual, on purchasing a property, becomes a member of the property management company and all members of that company are entitled to receive account details relating to all other members of the management company. Of course, such lists are often circulated to embarrass the people involved into paying outstanding fees. In some complaints to our Office, the named individuals had in fact paid the fees in question.

In June 2010 we received two complaints against a property management company. The complaints alleged that the company disclosed the management fees owed by members. The complainants supplied us with a copy of a letter that issued from the company to its members. It enclosed a debtors list of members detailing the house number, the individual's first initial, surname and the amount of arrears in each case.

We wrote to the property management company asking that it outline the legal basis for sending this correspondence. The management company asserted that its Memos and Articles of Association provided for its members to have access to the company accounts and, therefore, to have access to creditor and debtor lists. On examining the text in the Articles of Association under the heading 'Accounts', we informed the company that it did not provide for the disclosure of management fees owed by individual members of the company. The text only provided the directors of the company with the right to decide on the availability of the accounts for inspection by members. We informed the company that the right to inspect the accounts was an entirely different matter to the circulation of details of management fee arrears to the company's members.

The company did not provide evidence that property owners consented to the circulation of personal information relating to the status of their management fees. In the absence of evidence of consent, we informed the company that it had breached the Data Protection Acts. The company provided us with letters of apology for each of the complainants to amicably resolve the complaints. In these letters the company acknowledged that it had breached the Data Protection Acts when it sent letters informing members that the complainants were in arrears with their subscriptions and gave an assurance that it would not happen again.

We expect property management companies to observe the law when processing the personal information of their members. In particular, they should note the following:

- Personal information in relation to individual property owners, as members of the management company, should not be circulated to other members of the management company unless the consent of the individuals concerned has been obtained.

- The entitlement of members of a management company to receive information in relation to the overall financial status of the company by means of annual audited financial reports (which is lawful) is an entirely different matter to the circulation by the company of details of management fees owed by individual members who have not consented to the circulation of their personal data (which is unlawful).

A Board of Directors or other executive body with legal responsibility for the management company has a legitimate basis for taking appropriate action on foot of an examination of a list of members whose management fees are in arrears. However, the broader disclosure of such a list to members who have no such legal responsibility breaches the "need to know" principle of the Data Protection Acts.

Part 3

Guidance

Revised breach notification guidance:
http://www.dataprotection.ie/docs/08/07/10_-_Breach_Notification_Guidance/1085.htm

Revised data security guidance:
http://www.dataprotection.ie/docs/Data_security_guidance/1091.htm

Employee vetting guidance:
http://www.dataprotection.ie/docs/Guidance_Note_on_data_protection_considerations_when_vetting/1095.htm

Appendices

Appendix 1 – Insurance Link Investigation

Appendix 2 – Presentations

Appendix 3 – Registration statistics

Appendix 4 – Account of income and expenditure

Appendix 1

Insurance Link

An investigation by the Office of the Data Protection Commissioner into the use of 'Insurance Link' by the Insurance Sector in Ireland

March 2011
Office of the Data Protection Commissioner

Contents

Executive Summary

In August 2008 the Data Protection Commissioner approved a Data Protection Code of Practice for the Insurance Sector. This Code was drawn up in recognition of the extent of personal data held and processed by the sector in the course of its business. The Code was accepted by a large number of insurance companies that sought to implement its provisions in their business processes, although the sector itself felt unable to accept it via its representative body.

The Code of Practice did not address the databases operated by the industry that allow for the sharing of information between them. It was felt that this area merited detailed examination in its own right. Nevertheless, the basic principles to ensure that the operation of such databases was in compliance with the Data Protection Acts were set out broadly in the Code.

The first database examined is known as 'Insurance Link' and the results of that investigation are detailed in this report. We will also examine the compliance of the operation of the well-known 'Insurance Confidential' system, a system for whistle-blowing in relation to alleged insurance fraud.

Insurance Link is a database that holds data in relation to claims submitted under the terms of insurance policies. A database such as Insurance Link, which provides for sharing of personal data between multiple entities inside and outside the insurance sector, can involve a significant setting aside of an individual's right to the protection of their personal data. The basis put forward for this 'set aside' is the legitimate interests of the entities involved in managing insurance claims and the fact that within the insurance sector the individual signs an authorisation for such use. However, the Data Protection Commissioner must also give consideration to the fact that only a small minority of people submit fraudulent insurance claims. A solution which provides for the sharing of over two million records may be deemed to be excessive in that context. As a consequence of this investigation the Data Protection Commissioner conveyed his concerns to the sector about the proportionality of the database and the continued justification for its operation. The sector will be required to continue to justify the necessity for a database of this nature.

In response, the insurance sector (through its representative body, the Irish Insurance Federation – IIF) indicated that "it needs to be borne in mind that insurance pools risk within the community for the provision of common welfare. The system is vulnerable to fraud. Such fraud can run to hundreds of thousands of euro for an individual claim. Its cost, when it occurs, is never borne by the shareholders of insurers and other entities involved in managing claims but rather by policyholders who must pay higher premiums as a result. Therefore Insurance Link must not be seen as something that defends the 'industry's interest'. The pooled / community based nature of insurance means that it is the community of the insured whose interests are protected by the database."

Even if the database is considered to constitute a proportionate and legitimate response to fraudulent claims, it is imperative to ensure that the use of such a database is in keeping with the highest data protection standards. This is the minimum expected. In response, the IIF indicated its agreement that adherence to such standards must be a condition of use of the database and also accepted that these standards have not been met by all users of the system. This is welcome.

This investigation has shown that many users of Insurance Link appear to have viewed their access to this massive holding of personal data as a right without corresponding responsibilities. They often paid scant, if any, regard to data protection requirements. No examples of best practice were found in any entity investigated. While some entities were certainly better than others, in most cases no evidence was found of anything beyond lip service to data protection requirements. For example, while the Insurance Link system contains an easy-to-use tool to monitor employee access to the system, this tool was not used in any meaningful way by members. Indeed, in some cases, they were completely unaware of its existence. In one case the user believed that it was the responsibility of the system provider to check such access.

It may not be well known that membership of Insurance Link is also open to organisations who self-insure against certain risks. It was therefore also necessary to examine the use made of the system by these entities. By coincidence these entities had just begun accessing the system online. Therefore the investigation provided a timely focus on avoiding the mistakes made by the insurance companies. The previous paper-based means of accessing the claims information on Insurance Link had its own in-built privacy protection. It required a time-consuming paper trail which ensured that there was no real possibility of inappropriate access. The availability of such information at the click of a button provides no such protection.

By and large we received full co-operation with our investigation from the IIF and individual insurance companies. The self-insured entities that have access to Insurance Link adopted a more challenging approach via their co-ordinating group, the Self-Insured Taskforce. In the course of our engagements with them they put forward a number of points which are reflected in this report. One self-insured member put forward the argument that data protection law did not apply to certain aspects of their use of the database and initially refused to provide a response to the Office. The approach of the Taskforce to our investigation was surprising given that the justification for their access to Insurance Link is much weaker than that of insurance companies. The issue of the continued access of the self-insured to Insurance Link needs to be considered further.

While the Commissioner is satisfied that none of the investigated entities deliberately sought to breach the provisions of the Data Protection Acts through their use of Insurance Link, the actions and inactions of a number of members of Insurance Link served to breach the Acts on a major scale. The purpose of this report is to make the requirements of the Data Protection Acts in this area as clear as possible. We expect all members of Insurance Link to amend their procedures immediately in accordance with its recommendations. We will scrutinise implementation of the recommendations closely.

Key Recommendations

Obtaining and Processing of Personal Data & Purpose Limitation

- The upload of pre-claims data to Insurance Link should cease immediately and all pre-claims data previously uploaded onto Insurance Link must be removed from Insurance Link by each member of Insurance Link within an agreed timeframe.

- The practice whereby claims handlers conduct checks on Insurance Link based on pre-claims notifications data without adequate justification must cease immediately.

- Insurance Link must be directly referenced on relevant documentation used by insurance companies and the self-insured. A contact point must be provided for all queries in relation to it. It should be clear to the claimant that their claim will be/was placed on Insurance Link.

- The existence of Insurance Link should be explicitly highlighted on a dedicated website providing full transparency and a central means for individuals to access their data if they wish to do so. In addition, it should be directly referenced on the Irish Insurance Federation website. The IIF has indicated that this will be in place by mid-April 2011.

- This Office does not consider the use of Insurance Link at policy quotation stage to examine personal data to be legitimate in current circumstances. Those engaging in this practice must cease it immediately. The IIF has advised its members accordingly. Appropriate provisions and safeguards, to be agreed with this Office when the requirements of this report have been met, may alter circumstances to the extent that such processing can take place legitimately.

Further Processing/Disclosure

- Files held by an insurance company relating to a claim made by an individual should only be released to another insurance company or self-insured entity on foot of a Court Order or the explicit consent of the data subject on the basis outlined in the report. This Office has already engaged with the IIF and the Self-Insured Task Force on this matter and further discussions will take place in relation to explicit legal avenues that may be available for such disclosures.

Security

- Each member needs to instigate a programme of pro-active monitoring of all access within their organisation to Insurance Link. All users of Insurance Link should be made aware of these random spot checks and the consequences should inappropriate employee access be detected.

- The designated point of contact for each member should run a quarterly report detailing all users who have not accessed the service. Such reports

enable each member to identify redundant users in an effective and timely manner and to implement the necessary changes to access rights.

- Consideration must be given to the different requirements of each type of user approved to use Insurance Link. Their access privileges to personal data should reflect these requirements. The extent of each user's access privileges should be reviewed on a regular basis. Individual staff members should only have access to data which they require to perform their duties.

Adequacy, Relevance

- The upload of actual amounts paid in claims should be discontinued and any such data entered on Insurance Link should be deleted.

Retention Policies

- All personal data over ten years old on Insurance Link must be removed other than in exceptional circumstances (such as ongoing claims/litigation). In such exceptional circumstances, an active step should be necessary to extend the retention period.

Access Rights

- Members of the public must be made aware of their right to obtain a copy of any data held about them on Insurance Link.

General Matters

- A training structure to draw attention to requirements under data protection legislation should be in place at induction stage for all employees. Further opportunities to develop knowledge of data protection and privacy issues should be on offer at various stages throughout an employee's career. Particular emphasis should be placed on safeguarding customer data and the importance of access for business purposes only.

- All members need to put in place focused internal guidance/procedures clearly setting out the appropriate use and purposes of Insurance Link within each organisation. These procedures must clarify when it is, and is not, legitimate to access the system. The procedures also need to remind users that monitoring arrangements are in place for user access and that failure to follow the procedures could result in disciplinary action.

PREFACE

This report is intended to serve as a guidance document to ensure that practices within the insurance claims handling sector regarding access and use of the Insurance Link database are in line with the requirements of the Data Protection Acts 1988 & 2003.

Insurance Link is a shared claims database first developed in 1987 as a facility to allow 'members' of Insurance Link to upload, share and cross-reference individual insurance claims with other participating members. Insurance Link is intended to be used by insurance companies and self-insured entities to check, each time an individual makes an insurance claim, whether the individual concerned has any previous claims history. If a member runs a search on a claimant, summary details of any previous claim(s) in relation to the individual will appear in the search results. The industry considers that this data may be of relevance or interest in the context of a claim being handled by an insurance company. It is also possible to search the database using a range of other criteria such as address, surname, vehicle registration number etc (depending on authorisation levels). This allows information on individuals to be accessed relatively easily. Such broad access requires appropriate access control and monitoring policies.

1. INTRODUCTION

The Office of the Data Protection Commissioner conducted a series of general compliance audits[§§§] across the insurance sector between 2007 and 2009. This led to a more targeted series of investigations in 2010 based on serious concerns about the compliance of the operation of Insurance Link with the Data Protection Acts.

Issues with regard to Insurance Link were also identified as a result of intensive engagement with the insurance sector to draw up a Code of Practice aimed at ensuring compliance with the Data Protection Acts. Ultimately the Code was not endorsed by the Irish Insurance Federation, the key representative body for the insurance sector. Nevertheless, the Data Protection Commissioner formally approved the Code of Practice for the Insurance Sector in 2008 and promoted compliance with it throughout the sector.

1.1 Who uses Insurance Link?

In addition to commercial insurers, loss adjusters and specialist underwriters operating in the Irish insurance market, authorised 'members' also include self-insured entities such as local authorities and a department store. All members signing up to use Insurance Link are pre-approved for membership by one of two representative bodies: the Irish Insurance Federation or the Self-Insured Taskforce.

1.2 Membership

[§§§] Compliance Audits conducted by the Office of the Data Protection Commissioner consist of a review of an organisation's compliance with the Data Protection Acts 1988 & 2003 in selected areas chosen for inspection, in addition to an assessment of the organisation's level of awareness regarding data protection requirements based on existing policies and practices within that organisation.

Insurance Link Members

Axa
Allianz
Aviva
FBD
Royal Sun & Alliance
Aon
Irish Insurance Federation
Irish Public Bodies Taskforce
Chartis
Sertus
Travelers Insurance
MIBI
Quinn Insurance
Zurich Insurance
Kennco Underwriting
OSG
Prestige Underwriting
Cunningham & Lindsey
ProAdjust
Thorntons
South Dublin County Council
Fingal County Council
Dublin City Council
Cork City Council
Limerick City Council
ESB
CIE
Dunnes Stores
Arnold & Green
Orr & Company
Dooley Car Rental

1.3 Management and Hosting of Insurance Link

The Insurance Link database is currently hosted by Risk Intelligence Ireland, an Irish-owned company that primarily develops financial reporting software for financial institutions. Risk Intelligence Ireland (RII) manages and hosts the service on behalf of the two representative bodies and their members.

Terms and conditions of usage are outlined in a 'Customer Licence Agreement' drawn up between RII and each subscriber to Insurance Link. The IIF has responsibility for Insurance Link; it is the entity that selects the operator of the system in a public tender competition. By acting as agents under contract for these bodies, RII is deemed to be a 'data processor' in terms of data protection legal responsibilities. All members of Insurance Link are considered to be individual 'data controllers' in their own right.[****] This means that responsibility in relation to the legal use of the personal data on the database rests with the individual members supplying the data. RII has responsibility only in relation to the security of the data it holds.

[****] http://www.dataprotection.ie/docs/Are_you_a_Data_Controller?/43.htm

In 2006 a major upgrade to Insurance Link allowed members to access the database via a web portal. The Insurance Link web site went live for commercial insurers in March 2006 and for self-insurers in January 2010.

2. INSURANCE LINK DATABASE

2.1 Use and Purpose of Insurance Link

As of 12 November 2010, the Office of the Data Protection Commissioner established that there were 2,441,838 claim records on Insurance Link.

The stated 'raison d'etre' for the Insurance Link database is fraud prevention. In the course of the investigation representatives from the sector indicated that the search results do not provide any indication of specific fraudulent claims to members. Instead the results are intended to provide members with information that may support a decision to make further enquiries concerning a particular claim.

The principle of 'reciprocity' is at the centre of this system. Members must agree to upload all claims data that they receive, thus ensuring that Insurance Link is updated on a regular basis with the latest claims data. In a typical scenario an individual suffers some type of injury or their insured property is damaged or stolen and they make a claim. The fact that the individual has made a claim against a particular insurance company is recorded and uploaded onto Insurance Link by their insurance company or by the entity from whom they are seeking compensation e.g. their local authority. In return for regular uploads of claims data, members are able to search and view details of claims uploaded by other members. Participants can only view the same amount of detail as they themselves upload onto the database.

Search results on Insurance Link may also lead to examination of information provided at policy proposal stage by the claimant. In some instances the claim may not be paid if it is concluded that information materially relevant was not disclosed at proposal stage.

Users can search Insurance Link under four categories of claim accessed from a drop down list - motor, property, injury or all.

> The system groups the claim types into the following:
>
> **ALL:** Search all claims pooled in the system.
>
> **PROPERTY DAMAGE:** Search the property damage claims (household, motor damage) in the system.
>
> **INJURY:** Search the injury claims (personal/motor injury, employer liability, public liability) in the system
>
> **MOTOR DAMAGE:** Query the motor damage claims (write off, damages, stolen) in the system.

2.2 Conduct of Investigation

This Office began its investigation by conducting a detailed audit of Insurance Link at the premises of RII. On foot of that audit all claims data uploaded and accessed on Insurance Link in March 2010 was provided on request to the Office of the Data Protection Commissioner. In addition, the details of all authorised users were provided. We used this information to identify access by each member of Insurance Link and also to identify patterns of access and extensive non-use by those authorised to use the system.

In May 2010 the Office of the Data Protection Commissioner wrote formally to almost all members of Insurance Link (*i.e.* entities who subscribed to Insurance Link). The letter outlined the concerns of the Office that:

- the current level of access to Insurance Link by members is excessive taking account of the 'need to know' access principle;

- data in relation to pre-claim information is being entered on the database in advance of the confirmation of an actual claim;

- users are accessing claim data on the insurance link system for purposes that are not covered by the consent obtained from individuals when such data was placed on the database;

- there is a lack of oversight to ensure that all access by authorised users is for authorised purposes;

- there is no discernible policy in relation to the removal of personal data from the system after a specified time.

To assist the Office in forming a view on these matters all members of Insurance Link were asked to provide the Office with a detailed set of data, files and documentation concerning claim details and internal procedures and processes by the middle of July 2010 (the letter is reproduced at appendix 1).

As detailed in the statistics below, 19 of the 26 organisations had to be contacted again in relation to the datasets and documentation provided in their initial response (A sample of the letter issued is reproduced at appendix 2).

This report has been structured to map the investigation and findings directly against the 8 key data protection rules set out in the Data Protection Acts 1988 and 2003.

Insurance Link Investigation - Statistics		
How many companies did we write to?	26	
How many replied on time?	20	(77%)
How many did we have to further revert to?	19	(73%)
How many did we arrange to visit?	5	(19%)
Number of entries on IL database:	2,441,838	
Number of staff accesses in March 2010:	27,583	
Number of staff authorised to access IL:	1,725	
Number of staff who accessed IL in March 2010:	658 (38% of users)	

3. 'Fair Obtaining & Processing' and 'Purpose Limitation'

3.1 Fair Obtaining & Processing

> "the data or, as the case may be, the information constituting the data shall have been obtained, and the data shall be processed, fairly"
>
> - section 2(1)(a) of the Data Protection Acts 1988 & 2003

'Fair obtaining and processing' is a fundamental principle of data protection. In essence it means that an organisation collecting personal data must collect and use the information fairly.

As part of the investigation, a review was conducted of members' claim forms. We note that this is not always available as an option for communicating with individuals as such forms are not used in certain circumstances. However, where they were in use, this Office did not consider that sufficient information was provided at claim initiation stage about the practice of checking and recording the claimant's details on Insurance Link. It was frequently termed a "sectoral database aimed at preventing fraud" or “insurance industry databases for the prevention of fraud”. This information or description is insufficient to inform an individual about the use of their personal data. The IIF in response has accepted that appropriate notification about this use must be provided.

This Office expects 'Insurance Link' to be directly referenced on relevant documentation used by insurance companies and the self-insured in the claims handling process. A contact point must be provided for all queries in relation to Insurance Link. It should be clear to the claimant that their claim will be/was placed on Insurance Link. We expect language of the following nature (adapted from a pre-existing data protection statement on Quinn Insurance’s website):

> “we share and exchange all claims information with the Insurance Link database, run by the Irish Insurance Federation. The aim is to help us check

> information and to prevent fraudulent claims. When you tell us about an incident, we will pass information about it to this register"

A statement of this kind should be accompanied with contact details if more information is required on Insurance Link, including a dedicated web address for Insurance Link.

In relation to the fair processing of claims information gathered by self-insured entities, the position was even less satisfactory. In many cases self-insured companies do not provide any information about the upload of personal data to Insurance Link. Therefore all information gathered in this manner is uploaded in breach of the Data Protection Acts. Even where information about the database was provided it was, at best, basic and did not meet the requirement for fair processing. The self-insured sector expressed the view that the upload of claims data to Insurance Link did not need to comply with data protection requirements on the basis of a provision in section 30 of the Civil Liability and Courts Act 2004. This provision relates to court settlements of injury claims. This Office notes that the provision in question has not yet commenced (a statutory order is required). In any case, it does not appear to be relevant. The self-insured sector must immediately put in place appropriate provisions to meet the requirements of the Data Protection Acts in this area. We welcome the sector's commitment to provide appropriate information to claimants in this regard.

The Data Protection Commissioner also recommends that the existence and purpose of Insurance Link should be directly referenced on the Irish Insurance Federation website and that a dedicated Insurance Link website should be put in place providing information about the database. This will ensure transparency in regard to the purpose and use of the system. It will also allow data subjects to exercise their rights of access under section 4 of the Data Protection Acts. We consider that this increased transparency will also serve the interests of Insurance Link members, as increased knowledge of the database may constitute a disincentive to insurance fraud.

3.2 Collection and Upload of "Pre-Claims" Data

The Office of the Data Protection Commissioner has a specific concern about the inclusion of data in relation to pre-claim information on the Insurance Link database in advance of the receipt of a claim. The practice whereby pre-claims data is recorded and uploaded onto Insurance Link breaches the fair processing requirement of the Data Protection Acts 1988 & 2003.

The Code of Practice for the Insurance Sector made clear reference to this practice and advised that

> "Insurance policies should not other than in compliance with a specific legal obligation such as that contained in the Road Traffic Acts, as a condition of the policy, require the provision of personal data of potential claimants at a pre-claim stage of any incidents, e.g. workplace accidents that might lead to a claim. Where notification is required of incidents that fall within the scope of the policy, this should take place by the provision of anonymised data only, except where there is clear evidence that a claim is likely to be made by the subject(s) of the report."

In early 2010 the Office conducted an audit of FBD Insurance. We obtained clear evidence that pre-claims data was being uploaded onto Insurance Link. We have no reason to believe that FBD was unusual in this regard. We consider that FBD was not deliberately seeking to upload pre-claims data; in fact its systems did not distinguish between actual claims and pre-claims data. A subsequent audit of Allianz confirmed that it was also unable to distinguish on its systems between pre-claim and actual claims data for the purpose of uploaded the data to Insurance Link.

Based on the findings of other ODPC audits[††††] concerning the disclosure of personal details of individuals to insurance companies by insured parties, this Office formed the view that sharing of pre-claims data via Insurance Link was prevalent throughout the sector. Physical examination of files in several separate audits of insurance companies and detailed interviews with claims assessors as part of the Insurance Link investigation confirmed that this practice was widespread.

We discovered many cases of data subjects that were not aware that their data was notified by an insured party to an insurance company. For example, this included

> *"an incident report form containing the personal details of a customer who slipped in the aisle of a supermarket. The customer completed the incident report form for the supermarket providing their name, address, phone number and date of birth on the form unaware that this data would be passed by the supermarket onto its insurer and uploaded onto Insurance Link regardless of whether or not the customer went on to pursue a claim."*[‡‡‡‡]

We also encountered cases of insurance company customers who contacted the company regarding their policy and the implications of making a claim (no claims bonus, excess on policy etc). As a result of the information provided by the insurance company, the customer may have decided not to proceed with the claim. In some instances, the information provided by the customer was recorded and processed as a matter of procedure as if it were an actual claim and the details were uploaded onto Insurance Link.

The upload of such pre-claims data can create problems for the relevant individuals should they subsequently make a legitimate claim on another matter. In such cases the "pre-claim" would be listed as a claim. The individual may be considered to have withheld a material fact when taking out insurance cover because of the listing of the non-existent claim.

An audit of one insurance company revealed that some 30,000 pre-claims were loaded onto Insurance Link without a valid basis. The company, on discovering this, acted immediately to remove all these records.

Recommendations

[††††] The Office raised the issue of accident and incident report forms in a number of previous audit reports outside of the insurance sector. These included audits of a transport authority and several grocery retailers. In these cases the incident report forms were being passed onto commercial insurers as a condition of the terms of insurance (where the insured party estimated that certain thresholds had been exceeded). These report forms contained the names and addresses of the person(s) involved in the incident in addition to the names and contact details of witnesses.

[‡‡‡‡] Extract from 2009 audit of a supermarket

The practice of obliging insured parties to report pre-claims data as part of their terms of insurance is not in accordance with the Data Protection Acts. The disclosure of the personal data of third parties by one data controller to another, when the data subject has not yet instigated a claim, is not in compliance with the Acts. Therefore, as the Insurance Sector Code of Practice states, only anonymised data should be required or accepted by insurance companies in these cases. The Office is engaging with the IIF on this issue with a view to reaching a shared understanding.

The practice of uploading pre-claims data to Insurance Link should cease immediately. All pre-claims data previously uploaded onto the database must be removed by each member of Insurance Link as soon as possible. This will be the subject of further examination by the Office.

Claims handlers must immediately cease conducting checks on Insurance Link based on pre-claims notifications data without adequate justification.

4. Purpose Limitation

> "the data shall have been obtained only for one or more specified explicit and legitimate purposes"
>
> - section 2(1)(c)(i) of the Data Protection Acts 1988 & 2003

Under the Data Protection Acts 1988 and 2003, there must be specific, clear and legitimate purposes for collecting personal data and customers have a right to be informed of those purposes. The personal data sought and kept by data controllers should be sufficient to enable them to achieve their stated purposes and no more. It is therefore unlawful to collect and record information about people routinely and indiscriminately without having a sound, clear and legitimate purpose for so doing.

With regard to this investigation, the concern we raised in our initial communication with Insurance Link members was that the system was being used for purposes beyond the consent originally obtained from the relevant individuals. This usage could include searching Insurance Link at underwriting stage, accessing Insurance Link without any claim or notification having been instigated, or uploading the personal data of individuals onto Insurance Link at pre-claim stage.

During the investigation we became aware that a small number of insurers were accessing Insurance Link before giving policy quotations. Based on our examination the practice was not widespread. However, where it occurred we received no information to suggest that consent was sought and obtained from customers prior to accessing their information at quotation stage. It is our view that such access to Insurance Link at policy proposal stage is in breach of the Data Protection Acts. The issue of accessing Insurance Link at quotation stage was discussed with the Office in 2004 but was not followed-up in any meaningful way by the insurance sector. At the time it was accepted that the sector had an arguable justification for the use of the database at quotation stage but it was necessary to obtain consent. In the meantime sector-wide efforts were not made to collect consent from individuals at the time their details were collected (some insurance companies did do so but the majority did not). Therefore the legitimacy of now collecting a retrospective consent to access information as a condition of a quotation is extremely doubtful. A consent given in such circumstances, where there is no real alternative for the individual, would lead to justifiable questions as to whether the consent could be considered to be freely given. Another issue is that Insurance Link also contains information provided by

self-insurers who in most instances have not provided any real information to claimants as to the use of their information.

Recommendation

The use of Insurance Link at policy quotation stage to examine personal data is not considered legitimate in current circumstances. Those engaging in this practice must immediately cease. The sector may yet produce more concrete proposals on how such access can take place in compliance with data protection requirements. This will require demonstrable evidence that the sector has addressed the range of issues outlined in this report. In response to this issue the IIF has stated:

> "we have written to IIF users of Insurance Link informing them that they should immediately cease using the database at underwriting stage. We have advised them that this is not necessarily permanent but that any change in your view is contingent upon the development of new agreed (between the industry and ODPC) practices within the industry."

5. Further Processing/Disclosure

> "the data shall not be further processed in any manner incompatible with that purpose or those purposes"
>
> - section 2(1)(c)(ii) of the Data Protection Acts 1988 & 2003

This provision of the Data Protection Acts means that if an organisation obtains personal information for a particular purpose, the organisation may not use or divulge the personal data to a third party except in ways that are "compatible" with the specified purpose. A key test of compatibility is whether the organisation uses and discloses the data as those who supplied the information would expect it to be used and disclosed.

With regard to this investigation, the concern we raised in our initial communication to Insurance Link members related to the disclosure of personal data to third parties. The Office first became aware of the practice of disclosing data subject files to other insurance companies during the course of the investigation of a complaint from a member of the public. In September 2010, the Commissioner issued a decision on that particular complaint. His decision indicated that the insurance company in question contravened Section 2A and 2B of the Data Protection Acts 1988 & 2003 when it provided information relating to the data subject to another insurance company without a proper legal basis for doing so. The file was disclosed solely on the basis of a request from one claims handler in an insurance company to another claims handler in the other insurance company.

The complaint investigation established that sharing files following a "hit" on Insurance Link was common practice. For this reason the Office of the Data Protection Commissioner requested each member of Insurance Link to submit to the Office

> "a list of all files in relation to claims provided to other insurance companies, at their request, following a match by them on Insurance Link during March and the legal basis for the provision of such personal data in each case".

Responses from many Insurance Link members confirmed the disclosure of the personal data of previous or current customers to other insurance companies. These disclosures included verbal exchange of information over the phone, communication

of information by e-mail and the physical transfer of a copy of the entire file to the third party.

Some of the companies indicated that they could not provide documentary evidence of all disclosures made to third parties in March 2010 as there was no central list itemising disclosures of customer files to third parties. This was a further source of concern as it indicated that the relevant companies did not consider it necessary to control or monitor the disclosure of customer files (often including medical reports) to other entities. It appears that the decision to disclose was often left with individual claim handlers who were not in a position to make an informed decision on the legal basis for such a disclosure. For example, we were disappointed to be informed by Quinn Insurance that a manual check had indicated that there was no record of any exchange of files during March 2010. In fact we had evidence of a request for a disclosure from Quinn to Cork City Council. The request was sent by e-mail in March 2010 and requested that the member

> "forward all documentation relating to this claim including any injuries sustained, solicitor involvement, medical reports and settlement details"

The request then went on to state that

> "the information is requested for the detection and prevention of fraud and sharing of this information is therefore allowed under the Data Protection Act"

We encountered another example involving an insurance company that e-mailed Cork City Council seeking the date of birth of a claimant whose details they had viewed in summary on Insurance Link. Cork City Council reverted the next day with details of a public liability claim taken by the individual, stating the claimant's date of birth and describing the injuries cited by the claimant as having been sustained.

This Office is concerned that, given the broad membership of Insurance Link, an exchange of data between members could mean the disclosure of information including sensitive personal medical data between a supermarket and an insurance company, a local authority and a transport company, or between a telecommunications company and an insurance company. In all instances the information disclosed would relate to a separate claim.

Recommendation
Personal information held by an organisation relating to a previous claim should only be released to another insurance company or self-insured entity on foot of a court order or the explicit consent of the individual. To clarify, explicit consent is the clear, unambiguous, freely given consent of the individual. It is possible that such consent may be obtained from the individual following a verifiable “hit” on insurance link as a condition of payment of a claim where an individual had not revealed a previous claim.

An insurance company must comply with a court order. This situation is provided for in Section 8(e) of the Data Protection Acts. A witness subpoena would not be a sufficient basis to disclose the data. The Office also wishes to make it clear that the investigation of fraud by an insurance company cannot be the basis for a disclosure to that company by another insurance company or any other entity under Section 8(b) of the Data Protection Acts. This basis can only be relied upon by a law enforcement authority.

This Office has engaged with the IIF and the Self-Insured Task Force on this matter and further discussions will take place on the legal issues involved.

6. Security

> "appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing"
>
> - section 2(1)(d) of the Act

As previously indicated, all members signing up to use Insurance Link are pre-approved for membership by one of the two representative bodies: the Irish Insurance Federation or the Self-Insured Taskforce. Specific conditions of usage are outlined in a Customer Licence Agreement drawn up between RII and each subscriber to Insurance Link.

In terms of members' general obligations with regard to security, the licence agreement stipulates that

> "The Member shall implement appropriate technical and organisational measures to safeguard the data from unauthorised or unlawful processing or accidental loss, destruction or damage including loss, destruction or damage caused by distributed denial-of-service attack, viruses or other technologically harmful material, and that having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the data to be protected."

Addressing data protection legislation specifically RII, as the contractor (and data processor), states that:

> "The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the Data Protection Legislation."

6.1 'Need to know' Access to Insurance Link

All data controllers have a duty to limit access to personal data on a "need to know" basis with greater access limitations and controls applying to more sensitive data. In terms of this investigation of Insurance Link, we placed a focus on access levels and authorisation levels for each subscriber to Insurance Link. We examined all searches conducted on Insurance Link in March 2010 for any evidence of inappropriate employee access.

Access Levels

There are two levels of access or types of user account within Insurance Link; these are "standard" and "management" access.

"Standard" access allows a claims handler within a member organisation to undertake searches of the Insurance Link database. However it is not possible to

search under name alone if operating with standard access. Surname and address are required as a minimum to perform a query. It is also possible for a user with standard access to perform a search using vehicle registration number only.

“Management” level accounts allow for 'complex queries' described as “a research tool for investigation units”. Complex queries allow a user to construct customised queries where there is no minimum amount of information required.

The specific concern we raised about data security in the initial letter issued to Insurance Link members was that "the current level of access to Insurance Link by members is excessive taking account of the 'need to know' access principle". For this reason we examined the extent of access levels within the claims areas of Insurance Link members. All members or subscribers to Insurance Link were asked to provide the Office with:

- Details of any discrepancy between the number of individuals with access to Insurance Link and the number who actually used the database during March, with an explanation of non-use by certain authorised users during this period;

- A copy of the internal procedures in place for approving and removing authorised users from Insurance Link.

Quinn revealed that 599 users had been allocated access rights to Insurance Link but that "of these users, 437 of the registered user names were not used to access the database in March". A breakdown was provided to indicate possible reasons for "nil usage" and strikingly 138 users had since left the company and access by 207 users "were not required for claims handled in March". In the case of Zurich, there were 118 authorised users but over half did not use it in March. In the case of FBD, which had 155 authorised users, over a third of its authorised users showed no activity. AXA had 202 authorised users and almost half did not access the system. These responses were not acceptable and identified serious deficiencies in policies and procedures. The companies failed to monitor or review their user-provisioning systems, thereby exposing their organisations to increased risk from a security perspective and exposing data subjects to an unacceptable risk of inappropriate access to their data.

Specific procedures sometimes referred to as "movers, leavers and joiners" policies are required in all organisations with access to personal data. These policies allow organisations to increase or restrict previous access when a user’s role changes. Such policies are also designed to prevent the use of shared credentials (multiple individuals using a single username and password) and detect any use of default passwords. However, these policies and procedures must be supported by regular reviews of actual access to ensure that all authorised access to personal data is strictly necessary and justifiable for the performance of a business function. Throughout the sector, almost without exception, no evidence was found of appropriate “movers, leavers and joiners” policies and access reviews in relation to Insurance Link.

Prior to the Insurance Link investigation, we were informed by RII that it had a single designated point of contact with each of the member organisations accessing Insurance Link. Each of these contacts must liaise with RII in relation to the setting up of individual user accounts and any technical issues. It was confirmed that new accounts can only be set up by RII; members cannot set up new users themselves. Members are requested to inform RII when a user no longer has a requirement to use Insurance Link.

There are technical mechanisms on Insurance Link to identify redundant user accounts. Management reports to support the user-provisioning process are available to members to run on the Insurance Link portal. These reports show user activity over a specified date range. If these reports were run by the designated point of contact on a quarterly basis, they could be used by each member to identify redundant users in an effective and timely manner.

Recommendations

The designated point of contact for each member should run a quarterly report to identify all users who have not accessed the service during that quarter. These reports will enable each member to identify redundant users in an effective and timely manner and to implement the necessary changes.

Based on the responses received it was also apparent that, in many instances, access is not limited to claims handlers working within the various insurance companies. Some members had also provided staff based in the underwriting section with access authorisations (see section 4 above in regard to purpose limitation).

6.2 Inappropriate Employee Access

In our initial letter issued to Insurance Link members we identified our concerns regarding inappropriate employee access to the system: “there is a lack of oversight to ensure that all access by authorised users is for authorised purposes".

All members or subscribers to Insurance Link were asked to provide the Office with:

- a copy of the internal guidance/instructions available to users informing them of the circumstances in which Insurance Link may be accessed;

- a copy of the internal procedures and processes for validating that access to Insurance Link takes place in line with the guidance/instructions issued.

In addition to conducting an examination of the written policies and procedures referred to above, we examined the claims search data for all searches conducted on Insurance Link in March 2010. We sought this data from each member to detect any evidence of inappropriate employee access.

Many of the data extracts initially submitted by the members in their responses did not contain a claim reference number. Upon inquiry, it was established that there was no facility to record the claim number on Insurance Link when making the search and so a column containing the claim reference numbers had not been generated in the reports produced (we welcome the action already taken to remedy this situation). We were obliged to write to Insurance Link members again seeking a more detailed dataset based on their own in-house systems. The datasets requested included the claim reference number, the specific search criteria used, the number of hits (if any) associated with the search, the time and date of the search and the name of the employee conducting the search.

Our detailed analysis of the data confirmed our concerns about inappropriate employee access. Verified cases of inappropriate access to Insurance Link in

contravention of the Data Protection Acts 1988 & 2003 were identified in over 50% of Insurance Link members. Cases raising serious concerns were identified in most other insurance companies.

Commendably, several Insurance Link members conducted their own analysis of the dataset against internal claims references. They contacted our Office to inform the investigation team that, having examined the data and conducted interviews with the relevant claims handlers, inappropriate access had been detected. In most cases, disciplinary action had already been initiated.

Examples of inappropriate access uncovered:

- One search conducted by an employee in Zurich Insurance was a search of a noted celebrity. This celebrity had not registered a claim and there were no previous claims recorded on Insurance Link;

- In several cases of suspicious searches with no claim number locatable, after further questioning by management employees admitted that the searches were for records of family members and friends. The companies informed us that "these searches were not in fact claims-related but were of a personal nature i.e. the individuals listed were friends of hers";

- An individual was searched by a number of employees at Aviva and FBD on the same day. The investigation team subsequently ascertained that this individual was involved in a prominent court case reported in all the national daily newspapers on the date in question;

- The victim of a car accident, a close family relative, and the defendants in the related court case all had their details searched by an employee in Quinn Insurance following newspaper coverage of the case;

- Two employees in Allianz searched the same person on the same day with no claim number locatable or associated with either search;

- One employee in Quinn Insurance searched several relatives with the same surname as the employee;

- Some companies admitted that Insurance Link was routinely used by employees to check the claims history of a vehicle before purchase;

- In another case an Allianz employee searched the address of a house for sale at the time on a number of property websites.

Searches of Vehicle Registrations with no Claim Number

Given the consistency of responses across the sector, we accept that many searches of vehicle registration number only were related to third party vehicles and genuinely associated with ongoing claims. It was demonstrated that technically these vehicle registration searches could not be electronically associated with internal claims files for the purpose of this exercise. However, this restriction has also made it impossible to ascertain which vehicle registration searches were genuinely connected with a claim and which were not. We recommend that amendments are made to internal systems and procedures to remove, or at least minimise, this risk.

The reason provided for one search without an associated claim number was that the search was conducted as a result "of a car seen driving erratically". When questioned, staff confirmed that this was likely an employee who had spotted a car driving erratically. This does not justify interrogation of the Insurance Link system since it is not the responsibility of individual claims handlers to investigate such matters.

Recommendations

We recommend that each member should initiate a programme of pro-active monitoring of all access to Insurance Link within their organisations. Each member should conduct frequent random checks of employees and assigned users at a local level. All users of Insurance Link should be aware of these random spot checks and the penalties for inappropriate employee access to data held on Insurance Link.

Consideration must be given to the different requirements of each type of user approved to use Insurance Link. Access privileges to personal data should reflect these requirements. The extent of access allowed should be set and reviewed for each user on a regular basis. Individual staff members should only have access to data that they require to perform their duties.

A training structure to draw attention to requirements under data protection legislation should be in place at induction stage for all employees. Further opportunities to develop knowledge of data protection and privacy issues should be on offer at various stages throughout an employee's career. There should be a particular emphasis on safeguarding customer data and the importance of access for business purposes only.

Both the IIF and the Self Insured Task Force have outlined proposed approaches to address these matters that we regard as acceptable.

7. Accurate and Up-to-date Data

> "the data shall be accurate and complete and, where necessary, kept up-to-date"
> - section 2(1)(b) of the Act

The accuracy of the data reviewed on Insurance Link was severely impaired by the existence of pre-claims data and the absence of any retention policy allowing for the cyclical removal of redundant or closed claims data (after an agreed time period).

In addition, the lack of a facility to record the claim number on Insurance Link when uploading datasets posed a significant challenge in establishing the veracity of a claim as opposed to a pre-claim or any other data source. As a direct result of the investigation, a significant change to the upload process for claims data is now in place. Claims data now requires a claim number to be entered prior to upload. This will greatly improve the transparency of the upload process.

Apart from ensuring compliance with the Acts, accurate and up-to-date personal information has additional significance for insurers; the data controller may be liable to an individual for damages if it fails to observe the duty of care provision in the Act applying to the handling of personal data.

8. Adequacy and Relevance

"the data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed"

- section 2(1)(c)(iii) of the Act

The Data Protection Acts provide that personal data kept by an organisation should be enough to enable it to achieve a stated purpose, and no more. Collecting or keeping unnecessary personal information "just in case" a use can be found for it in the future is not acceptable.

This requirement did not emerge as a focus of attention in relation to the data uploaded to Insurance Link because the datasets visible on Insurance Link are sufficiently brief, neutral and factual in nature. However, certain insurance companies initiated a pilot process of entering the amount paid in a claim on Insurance Link. We can find no justification for including these details and we have made this clear to the sector. We expect that this practice will be discontinued and that any such data already entered will be removed immediately. This is an example of the "function creep" to which such databases are prone; additional data is entered without any material case being made for the processing involved.

Recommendation

The upload of amounts paid in claims should be discontinued and any data entered on Insurance Link in this regard should be deleted.

9. Retention of Personal Data

"the data shall not be kept for longer than is necessary for that purpose or those purposes"

- section 2(1)(c)(iv) of the Act

Under data protection legislation it is illegitimate to hold personal data on a "just in case" basis. Insurance Link contains data going back to the establishment of the service in 1987. There is no retention policy in place in relation to personal data held on the system. Other than in exceptional cases, we consider that ten years is a more than reasonable period to hold personal data on the system. Even in the cases of individuals with a rich claims history, it is considered that a ten year view of such history would normally be sufficient.

Recommendation

All personal data over ten years old on Insurance Link should be removed, other than in exceptional circumstances (such as ongoing claims/litigation). In such exceptional circumstances, an active step must be necessary to extend the retention period.

10. Access Rights

Section 4 of the Data Protection Acts affords a data subject the right to obtain a copy of their personal data. This "right of access" is subject to a limited number of exceptions[§§§§].

Under section 4 of the Data Protection Acts, on making a written request, any individual about whom an organisation keeps personal information on computer or in a relevant filing system is entitled to:

[§§§§] http://www.dataprotection.ie/docs/Exceptions_to_the_Right_of_Access/78.htm

(a) a copy of the data;
(b) a description of the purposes for which it is held;
(c) a description of those to whom the data may be disclosed; and
(d) the source of the data unless this would be contrary to public interest.

An individual making an access request must:

- apply in writing;
- give any details necessary to help the organisation identify him or her and locate all the information held about him/her (e.g., previous addresses, date of birth, customer policy numbers); and
- pay an access fee if the organisation decides to charge a fee (this fee cannot exceed €6.35).

Based on our inspection we do not consider that the right of access by the data subject to their personal data held on Insurance Link is sufficiently highlighted or signposted.

Recommendation

Insurance Link must be directly referenced on relevant documentation and a contact point should be provided for all queries in relation to it. The existence of Insurance Link should be made explicit on a dedicated website providing full transparency and a central means for individuals to access their data if they wish to do so. Direct requests to RII would appear to be the simplest means to achieve this aim. In responding to the requests it would do so on behalf of the individual members on whose behalf it holds the data. Additionally, the Insurance Link database should be directly referenced on the Irish Insurance Federation website.

Findings

The lack of transparency with regard to Insurance Link outside of its immediate membership was a striking outcome of the investigation. The existence of a database containing information on almost two and a half million claims needs to be clearly referenced and signposted by the insurance sector to allow members of the public to easily obtain more information on Insurance Link and its purposes. This is especially the case when the data in question is used to make decisions in relation to individual data subjects. From the perspective of the rights and freedoms of the data subject, we consider that the activities of the sector with regard to the processing of claims data on Insurance Link are not sufficiently transparent to policy holders. It is also vital that members of the public should be aware of their right to obtain a copy of any data held about them on Insurance Link and to seek corrections if necessary.

The lack of transparency surrounding Insurance Link compares unfavourably with practice in other sectors. In the banking sector the credit worthiness of loan applicants is widely known to be available to the industry and members of the public alike through the Irish Credit Bureau[*****]. We expect this lack of transparency to be addressed immediately. In the absence of such transparency we are concerned that that the operation of the database is not in compliance with the Acts.

[*****] http://www.icb.ie

The indefinite retention of records on Insurance Link dating back to its inception in 1987 was another key finding of the investigation.

One factor contributing to the large number of the records held on Insurance Link was the practice of uploading notifications regarding accidents or damage to insured property or persons (referred to in the report as 'pre-claims') that did not actually become claims. Our report makes a number of recommendations regarding the cessation of this practice and the retrospective removal of all pre-claims data from Insurance Link.

Our investigation also placed a particular focus on access levels within each member organisation. We examined the number of authorised users on Insurance Link against their activity patterns during March 2010. We also sought documentation in regard to user provisioning and any policies designed to safeguard against inappropriate employee access. Some serious incidents of inappropriate access were identified during the course of the investigation, leading to internal investigations and disciplinary proceedings. Our report includes a key recommendation concerning access restrictions and the need for proactive regular checks by member organisations.

Finally, the investigation uncovered evidence that member organisations were sharing information about claims without the knowledge or consent of the data subject. The position of the Office of the Data Protection Commissioner as detailed in this report is that disclosures of this nature cannot normally occur without a court order or explicit consent.

Appendix 1

X Insurance Limited

Dear X

I am writing to inform you that the Office of the Data Protection Commissioner is commencing an investigation into the use by the insurance sector of the 'Insurance Link' database. This investigation is taking place under section 10(1A) of the Data Protection Acts, 1988 & 2003, which states that

"The Commissioner may carry out or cause to be carried out such investigations as he or she considers appropriate in order to ensure compliance with the provisions of this Act and to identify any contravention thereof".

The Office of the Data Protection Commissioner has carried out a number of privacy audits across the insurance sector which have highlighted potential concerns in relation to aspects of the compliance of Insurance Link with the Data Protection Acts. In brief this Office has formed a concern that:

- the current level of access to insurance link within members is excessive taking account of the 'need to know' access principle
- data in relation to pre-claim information sought by insurance companies is being entered on the database in advance of the confirmation of an actual claim
- access is taking place to the claim data on the insurance link system for purposes beyond the consent obtained from individuals when such data was placed on the database
- there is a lack of oversight to ensure that all access by authorised users is for authorised purposes
- there is no discernible policy in relation to the removal of personal data from the system after a specified time

To assist this Office in forming a view on the above matters I would ask you to provide this Office with the following information:

i. the claim details that provided the basis for each enquiry by your company on the Insurance Link database during March 2010. We are aware that in some cases this information request may be extensive.

ii. the claim details that provided the basis for the upload of each separate claim to Insurance Link during March 2010

iii. details of any discrepancy between the number of individuals with access to Insurance Link and the number who actually used the database during March. An explanation is required as to why certain authorised users did not access the system during this period.

iv. a copy of the internal procedures in place for approving and removing authorised users from Insurance Link

v. a copy of the internal guidance/instructions available to users of Insurance Link informing them of the circumstances when Insurance Link may be accessed

vi. a copy of the internal procedures and processes for ensuring that such access to Insurance Link takes place in line with the guidance/instructions at (v) above

vii. a copy of the information provided to claimants to legitimise the upload of their claim data to Insurance Link

viii. a copy of the internal procedures in place for the steps to be taken once a match is made on Insurance Link

ix. a list of all files in relation to claims provided to other insurance companies, at their request, following a match by them on Insurance Link during March and the legal basis for the provision of such personal data in each case

In relation to the information sought at (i)-(iii) above, your attention is drawn to the reporting tools available within Insurance Link to assigned administrators.

I would ask that you provide the information sought by 12 July 2010. I am to inform you that if your company considers itself unable to supply the above information, an Information Notice will be served under the provisions of Section 12 of the Data Protection Acts. Such Notices must be complied with or appealed to the Circuit Court within 21 days of receipt. I would also advise that this investigation is targeting the use of Insurance Link by all Insurance Link members.

Yours sincerely,

_____

24 May 2010

Appendix 2 - Sample of follow-up letters issued

X Insurance Limited

23 July 2010

Dear X,

Thank you for your response of 8 July 2010. There are some issues however on which this Office requires elaboration to further our investigation in this area.

The Office has reviewed the claim details that provided the basis for each enquiry by X Insurance Limited on the Insurance Link database during March 2010. It is noted that a substantial number of searches have 'unknown' claim numbers. Of the 2,951 queries, we are requesting you to provide us with the total figure of 'unknowns' amongst those queries and also a total figure for the number of queries that have a blank within the claimant no. field. (see for example line 989).

In addition, we are requesting that X Insurance Limited account for each query in the absence of any claim number prompting the enquiry. Also, it is noted that the list of queries made during March 2010 does not indicate which authorised member of staff queried the system in each instance and on which date during March. The name of authorised users who conducted the 'unknown' queries or 'blank' queries is also requested.

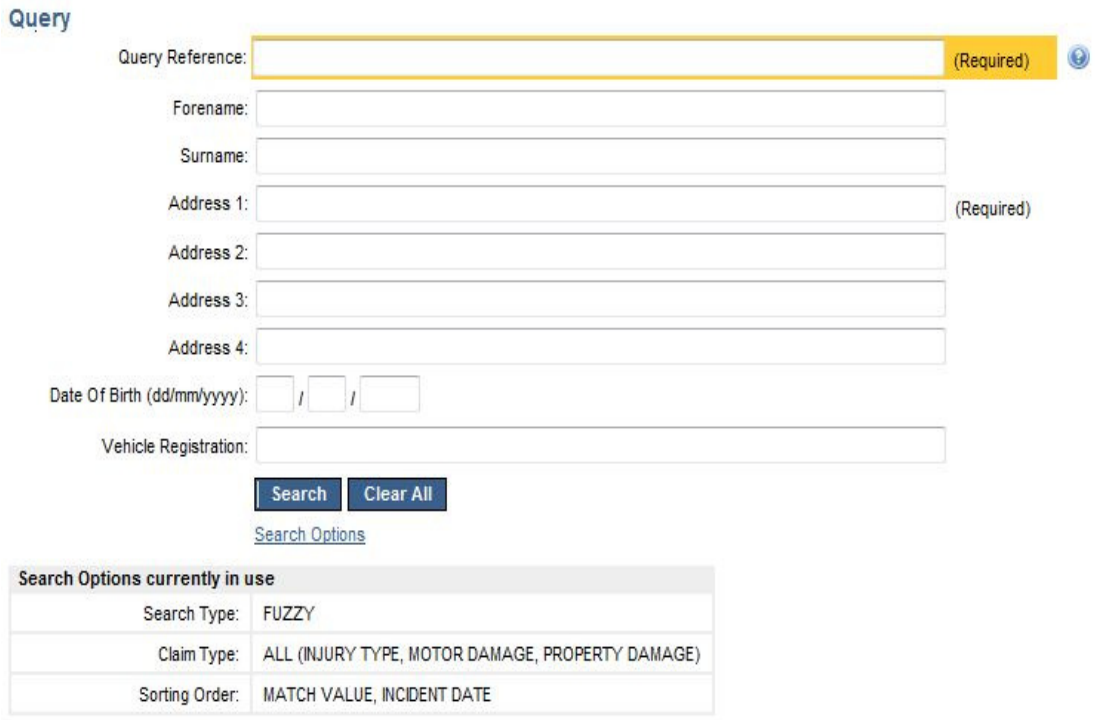
Finally, the Team notes the multiple queries under the same name alongside the claimant numbers that appear in the list provided and is unclear as to why there would be so many queries for an individual of the same name e.g. X Smith with each query appearing to pertain to a different claim given the claimant no. is different?

A response on the above is sought by c.o.b. 10 August 2010.

Yours sincerely,

_____

Appendix 3 Query Screen on Insurance Link



Appendix 4 Search Results Screen (A) on Insurance Link

Search Results

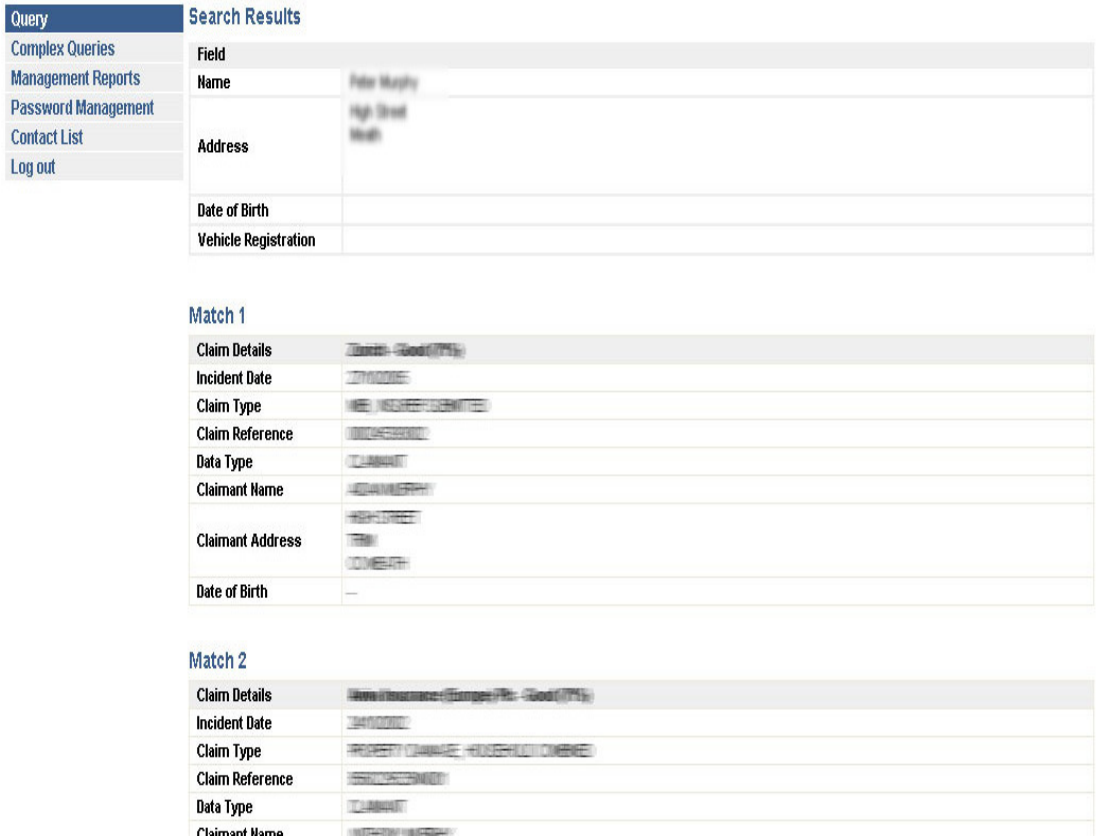
Field	
Name	[redacted]
Address	[redacted]
Date of Birth	
Vehicle Registration	
Query Reference	Claim Ref 297849035789

InsuranceLink Information

Member	Claim Type	Incident Date	Forename	Surname	Address Line 1	Match Quality
Aviva Insurance Europe SE	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Good (72%)
Zurich	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Good (66%)
Aviva Insurance Europe SE	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Good (66%)
RSA	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Good (66%)

Create Report | More Information | New Search

Appendix 5 Search Results Screen (B) on Insurance Link



Appendix 2 – Presentations and Talks

During 2010 my staff and I gave presentations to the following organisations:

Educational

Holy Secondary School x2
Waterford Institute of Technology
UCC
IVEA
Faculty of Public Health Medicine - Summer Scientific Meeting
Trinity College
Institute of Public Administration (IPA) x 4

Financial Services

Financial Services Ireland

Health Sector

HSE
National Treatment Purchase Fund
Ethics Committees Master Class
Home Care Ireland
HSE Child Care Services

International

Croatian Personal Data Protection Agency
European Data Protection Conference
Israeli Law and Information Technology Authority
Google
Facebook

Legal

Clare Law Association
Irish Human Rights Commission
Law Society of Ireland

Mixed Seminars

Association of Compliance Officers in Ireland
Cloud Consulting
Cork Chamber
Institute of International & European Affairs
Irish Computer Society
PDP DP Practical Compliance Conference x2
Public Affairs Ireland –Medical Records Data Protection
Public Affairs Ireland x 4

HSR Conference 2010
Legal Island Data Protection & Compliance Update Conference 2010
Institute of Leisure and Amenity Management Ireland

IRISS

Voluntary/Charity/ NGOs

Carmichael Centre
Irish Charities Tax Reform Group Annual Conference
Irish Council for Civil Liberties
Victims of Crime, Dept/Justice

Media

Press Council of Ireland

Government/Agency

Heads of Information Systems in Local Authorities Annual Conference
State Examinations Commission
Office of the Ombudsman for Children
Irish Sports Council

Appendix 3 - REGISTRATIONS 2010

The total number of register entries in 2010 was 4,954. This figure breaks down into the following categories:

(a) Financial and Credit Institutions
539

(b) Insurance Organisations
419

(c) Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts
77

(d) Telecommunications/Internet access providers
47

(e) Health Sector
1534

(f) Pharmacists
1132

(g) Miscellaneous
434

(h) Data Processors
772

Total number of registration entries:

2008	**2009**	**2010**
4156	**4318**	**4954**

In 2010 the number of organisations registered increased by 636 (approximately 15%). This increase reflects a greater awareness among data controllers of their obligations under the Data Protection Acts and a compliance drive by our office targeted at the medical sector.

Appendix 4 - Abstract of Receipts and Payments in the year ended 31 December 2010*

Receipts	**2009 - €**	**2010- €**
Moneys provided by the Oireachtas	1,814,553	1,449,329
Registration Fees	576,616	590,025
Other Receipts	2,201	39,643
Totals	**2,393,370**	**2,078,997**
Payments		
Staff Costs	1,352,133	1,282,087
Establishment Costs	161,738	151,060
Education & Awareness	0	0
Legal & Professional Fees	283,972	670††††††
Incidental & Miscellaneous	16,711	15,512
	1,814,554	**1,449,329**
Payments of Fees to the Vote of the Office of the Minister of Justice, Equality & Law Reform	578,817	629,668
	2,393,370	**2,078,997**

**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.*

†††††† This figure represents a substantial reduction in the payment of legal fees as a result of negotiated settlements, the award of costs etc.