An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

# Twenty-Fourth Annual Report of the Data Protection Commissioner 2012

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

**Index of Tables and Figures**

# Foreword

In last year's annual report, I referred to the increased pressure on the resources of our Office. I noted that this pressure was likely to increase under the "one-stop-shop" arrangement being proposed at EU level for oversight of multinational companies.

The Government has responded by providing additional staffing and funding. A recent statement from the Minister for Justice and Equality, Alan Shatter TD, further confirmed that: "*The Government, and I as Minister, will continue to keep the resourcing of the Office of the Data Protection Commissioner actively under review and will ensure that any additional necessary resources will be made available to the Office of the Data Protection Commissioner*".

We are therefore well-placed to discharge the additional responsibilities that arise for our Office from the increasing number of information-rich multinational companies that are choosing Ireland as a base from which to provide services on an EU-wide basis.

Our necessary focus on multinational companies has not led us to neglect our responsibilities in relation to domestic issues. The Report includes information on the extensive work carried out by the Office on data protection issues arising in many sectors. In most cases we succeeded in achieving compliance with the law by persuasion but, where necessary, we used our enforcement powers to the fullest extent.

The Report includes a special report on our extensive investigation of data sharing in the public sector through the INFOSYS system provided by the Department of Social Protection. The report reveals a disturbing failure of governance in some of the public bodies investigated. Data sharing can bring benefits in terms of efficient delivery of public services. But it must be done in a way that respects the rights of individuals to have their personal data treated with care and not accessed or used without good reason. The failures revealed by the INFOSYS audit need to be addressed on a public-service-wide basis before any other such sharing arrangements are put in place.

Proportionality is the key. Such data sharing in the public sector should have a clear basis in law; be clear to individuals that their data may be shared and for what purpose; have a clear justification for individual data sharing arrangements, with minimum data shared to achieve the stated public service objective; strict access and security controls; and secure disposal of shared data These principles are set out in more detail on our website.

The achievements during the year would not have been possible without the commitment and dedication of our staff. Such commitment was always evident in the work of Gary Davis, Deputy Commissioner, who left us earlier this year to pursue other opportunities. I wish him well.

*Billy Hawkes*
*Data Protection Commissioner*
*Portarlington, May 2013*

# Introduction

2012 was another busy year for our Office. Activity across our four main functions – Investigation and Enforcement, Guidance and Education, Audits/Inspections and Notifications (Registration) - increased significantly. The first prosecutions were taken against Telecommunications Companies for failure to comply with the new security and breach notification requirements under Statutory Instrument SI 336 of 2011.

Data protection issues related to the activities of multinational companies continued to absorb an increased amount of resources – especially the time of senior management. This increased activity put significant strain on our limited resources – an issue highlighted in last year's report.

**Allocation of Resources**

Note: Staff costs = 85% of Budget

| | |
|---|---|
| **Investigations & Enforcement**[1] | 35% |
| **Guidance & Education**[2] | 25% |
| **Audits/Inspections** | 15% |
| **Notifications**[3] | 10% |
| **EU/International Cooperation** | 10% |
| **Administration**[4] | 5% |

In recognition of the increased responsibilities which are likely to fall to our Office, when the legislative proposals on data protection currently under discussion in the Council of Ministers of the European Union and European Parliament are passed into law, extra staffing was allocated to the Office at the end of 2012. These resources included a Chief Technology Advisor and a Legal Advisor, as well as additional

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

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

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

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

administrative staff. The non-pay budget allocation to the Office for 2013 was also increased.

***Customer Service***

This year, once again, the Office continued to provide services to our customers, both data controllers and data subjects, by phone, in person, by email and by post. We responded to large numbers of phone calls to our Helpdesk from members of the public on a very broad range of issues, from access rights to registration obligations. Emails were the next most common method of contact. Approximately 9500 queries were dealt with in 2012 via our dedicated information email address – info@dataprotection.ie. In addition we received queries by post.

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

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

In the last 12 months, we have given 76 presentations to various organisations, details of which are available in Appendix 1– Presentations & Talks.

**Media Relations**

We continue to place great value on our interaction with the media as this provides a valuable platform for raising awareness among the public of data protection issues. Last year the Office dealt with some 430 queries from the media. This in part reflects the ongoing media attention around the world on our investigation and subsequent audit of Facebook-Ireland but domestically the media interest in data protection matters has also significantly increased.

**Irish Language Scheme**

Our most recent Irish Language Scheme under the Official Languages Act 2003 was put into effect in 2010 and will be in effect until October 2013. The scheme will fall for review during 2013. We continue to maintain our commitment to provide an effective service to our customers, including by providing comprehensive information on our Irish language website, www.cosantasonrai.ie.

**Governance**

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

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

## Complaints and Investigations

During 2012, the Office received 1,349 complaints which were opened for investigation. This was a new record high number of complaints and it compares with 1,161 complaints in 2011. For the sake of clarity, it is worth noting that 369 complaints related to one particular matter.

The number of complaints under the Privacy in Electronic Communications Regulations (S.I. 336 of 2011) is significantly up on recent years. In 2012 we opened a total of 606 complaints in this category reporting unsolicited direct marketing text messages, phone calls, fax messages and emails. This compares with 253 such complaints in 2011, 231 in 2010 and 262 in 2009. This marked increase is due to the 369 complaints in relation to one issue referred to above. A large portion of the complaints received in 2012 with regard to unsolicited electronic communications related to marketing text messages sent by businesses large and small trading in Ireland. During the course of our investigations of these complaints we often find that

the offending businesses concerned are unaware of the law which applies to such communications with regard to subscriber consent and the requirement to provide an opt-out mechanism in each marketing message. As stated in previous Annual Reports, our prosecution powers will be used against entities who continue to infringe the law. The Case Studies section of this Annual Report carries details of the types of prosecutions taken in 2012. In total there were 195 prosecutions against 11 entities.

Table 1 shows the breakdown of complaints by data protection issue. 606 complaints (approx 45%) concerned breaches of S.I. 336 of 2011. The remainder (approx 55%) relate to breaches of the Data Protection Acts, 1988 & 2003. Complaints concerning access rights accounted for approx 33% of the overall total. A total of 442 complaints about access rights were opened in 2012 compared with 562 in 2011 (which included 183 class action complaints), 308 in 2010, 259 in 2009, 312 in 2008 and 187 in 2007. This upward trend reflects a growing level of public awareness of the right of access to personal data. Table 2 gives details of the number of complaints received on an annual basis since 2003.

**Table 1 Breakdown of complaints opened**

2012 - Breakdown of complaints by data protection issue

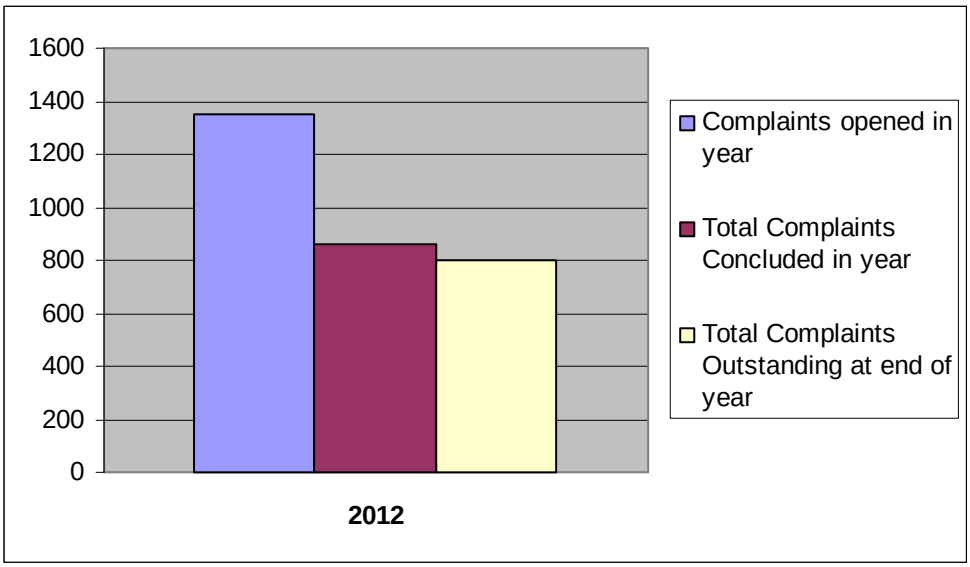
| | 2012 Percentages | Totals |
|---|---|---|
| Electronic Direct Marketing | 44.93% | 606 |
| Access Rights | 32.77% | 442 |
| Disclosure | 7.86% | 106 |
| Unfair Processing of Data | 2.59% | 35 |
| Unfair Obtaining of Data | 0.96% | 13 |
| Use of CCTV Footage | 2.37% | 32 |
| Failure to secure data | 2.59% | 35 |
| Accuracy | 1.41% | 19 |
| Excessive Data Requested | 1.78% | 24 |
| Unfair Retention of Data | 1.26% | 17 |
| Postal Direct Marketing | 0.74% | 10 |
| Other | 0.74% | 10 |
| **TOTALS** | **100.00%** | **1349** |

**Table 2 Complaints received since 2003**

| Year | Complaints Received |
|---|---|
| 2003 | 258 |
| 2004 | 385 |
| 2005 | 300 |
| 2006 | 658 |
| 2007 | 1037 |
| 2008 | 1031 |
| 2009 | 914 |
| 2010 | 783 |
| 2011 | 1161 |
| 2012 | 1349 |

As in previous years, the vast majority of complaints concluded in 2012 were resolved amicably without the need for a formal decision under Section 10 of the Acts or enforcement. In 2012, the Commissioner made a total of 36 formal decisions. 30 of these fully upheld the data subject's complaint, 2 partially upheld the complaint and 4 found that there was no breach of the law. A total of 864 investigations of complaints were concluded in 2012 (Figure 1).

**Figure 1 Complaints**




***Use of Statutory Enforcement Notices***

Details of Enforcement Notices and selected Information Notices served in 2012 are set out in the following tables. Most relate to the right of access. It is to be hoped that publication of these lists encourages all organisations that are the subject of complaints to co-operate fully with our Office in relation to our statutory investigations. While an Enforcement Notice may be issued in relation to a number of aspects of the Data Protection Acts, it is not normally necessary to do so. The vast majority of organisations voluntarily engage with the Office without the need for a formal legal notice to advance an investigation.

**Table 3 – Enforcement Notices* issued in 2012**

| Data Controller: | In relation to: |
|---|---|
| The Woodford Pub | Section 4(1) of the Data Protection Acts |
| Fleet Plan Hire Limited | Section 4(1) of the Data Protection Acts |
| M & A Couriers Limited | Section 4(1) of the Data Protection Acts |

| | |
|---|---|
| Sin Bar & Nightclub | Section 4(1) of the Data Protection Acts |
| JN Cummins (Engineering) Limited | Section 4(1) of the Data Protection Acts |
| Zevas Communications Limited | Section 4(1) of the Data Protection Acts |
| Munster Soft Drinks Limited | Section 4(1) of the Data Protection Acts |
| Nightline | Section 4(1) of the Data Protection Acts |
| SAS Institute Limited | Section 4(1) of the Data Protection Acts |
| Paintridge Limited | Section 4(1) of the Data Protection Acts |
| Paintridge Limited | Section 4(1) of the Data Protection Acts |
| Flexhaven Limited t/a Dinn Rí Hotel | Section 4(1) of the Data Protection Acts |
| Ashjen Limited t/a At Risk Security | Section 4(1) of the Data Protection Acts |
| Mason's Bar | Sections 2(1)(a) and 2(1)(c) of the Data Protection Acts |
| Tower Plant & Civil Engineering | Section 4(1) of the Data Protection Acts |

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

**Table 4 – Selected Information Notices* issued in 2012**

| Data Controller: |
|---|
| Scancor Limited |
| The Old Forge |
| SIPTU |

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

## Data Breach Notifications

During 2012, the Office dealt with 1,666 personal data security breach notifications. This is again an increase in the numbers dealt with compared to previous years. Of the 1,666 notifications received, it was found that 74 cases were not deemed to be personal data security breaches on the part of the data controller making the notification. This was due to either appropriate security measures, such as encryption, being in place to protect the data or to individuals failing to update their contact details with the data controller, resulting in letters issuing to an incorrect address. A total of 1,592 valid data breach notifications were therefore recorded. This is an increase of over 400 on last year.

The introduction, in July 2011, of S.I. 336 of 2011 made it a legal requirement for telecommunication companies and Internet Service Providers (ISPs) to notify this Office, without undue delay, of a data security breach and to also notify affected individuals of such a breach. In September 2012, two telecommunications companies were prosecuted for failing to meet their legal obligation in this regard. In the first full year of S.I. 336 being in effect, a total of 60 data security breach notifications were received from Telecommunications companies and ISPs.

Due to the year on year increase in the number of data security breach notifications received by the Office, additional resources were allocated to the area. A Technology Advisor has also been appointed to allow the Office properly investigate the more complex Information Technology (IT) related matters that are brought to its attention. During 2012, we have taken a more proactive stance in relation to potential data security breaches and have initiated investigations into matters that have been identified through mention in areas such as social media sites.

While the complexity of certain data security breaches increases, it is the more mundane situation of correspondence being issued to an incorrect address that continues to account for the largest percentage of data security breaches. Over two thirds of all breach notifications received by the Office involved letters being issued

by post (see Table 7), either to an incorrect address or containing a third party's personal data.

A new matter that is beginning to grow in terms of notifications is the issue of staff leaving the employment of one company and joining another, bringing with them the details of customers of their original employer. There are several facets to this issue. Firstly, the original employer has a duty under the Data Protection Acts to keep personal data under its control safe and secure. Secondly, the new employer can now hold personal data which it does not have consent to process. Thirdly, the new employer, in contacting these individuals, is potentially committing an offence under S.I. 336 of 2011 by sending marketing communications to non-customers from whom it does not have such consent. An example of this is set out in Case Study 14 in part 2 of this Report.

**Table 5 - Number of Breach Notifications received 2012**

| | |
|---|---|
| Total Number of Breach Notifications Received | 1666 |
| Number considered as non-breach | 74 |
| Number of Breach Notifications | 1592 |

**Table 6 - Number of Organisations making Breach Notifications, 2012**

| | |
|---|---|
| Private Sector Organisations | 220 |
| Public Sector Organisations | 84 |

**Table 7 – Breach Notifications – by Category**

| Category | Number |
|---|---|
| Theft of IT equipment | 30 |
| Website Security | 34 |
| Mailing Breaches (postal) | 1142 |
| Mailing Breaches (electronic) | 139 |
| Security | 46 |
| Other | 201 |
| Total | 1592 |

**Table 8 – Comparison of Breach Notifications – by Year**

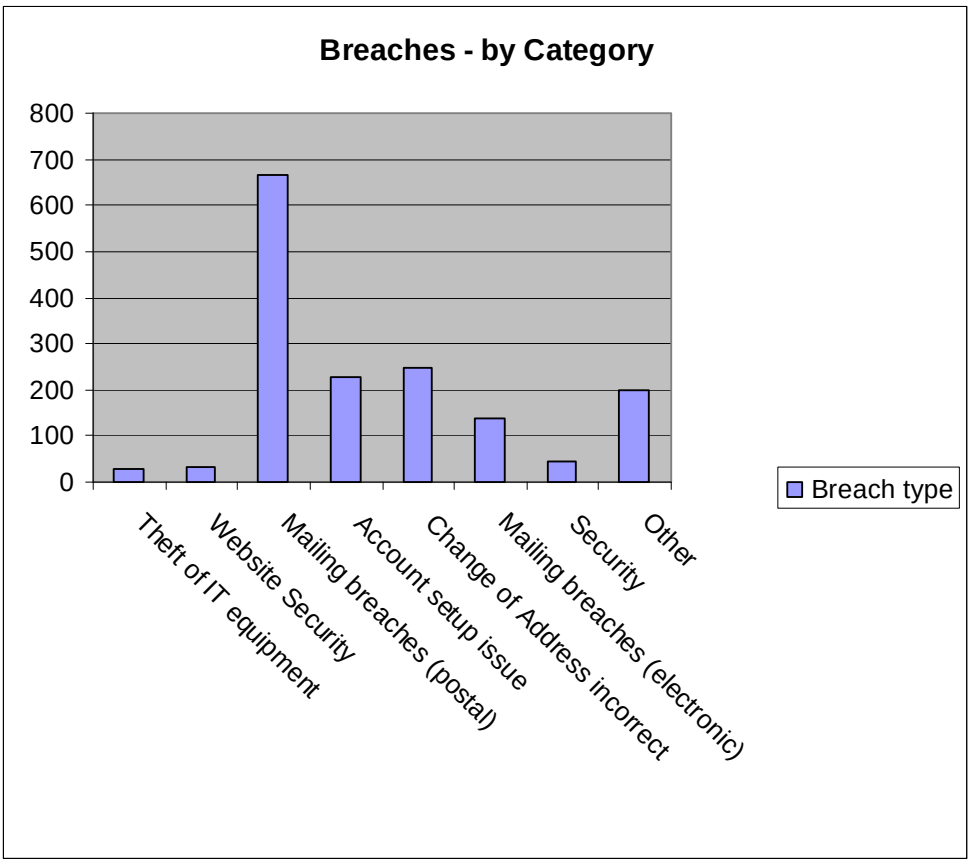
| | |
|---|---|
| 2009 | 60 |
| 2010 – introduction in July of Code of Practice | 410 |
| 2011 – Introduction in July of S.I. 336 | 1167 |
| 2012 | 1592 |

**Table 9 – Comparison of Organisations making Breach Notifications**

| Year | Private Sector | Public Sector | Total |
|---|---|---|---|
| 2009 | 60 | 26 | 86 |
| 2010 | 89 | 34 | 123 |
| 2011 | 146 | 40 | 186 |
| 2012 | 220 | 84 | 304 |

As can been seen in Table 7 above, postal breaches continue to account for the majority of breaches notified to this Office. Analysis of this issue showed that the majority of such notifications were received from the Financial Sector and that there were two readily identifiable issues which accounted for nearly 50% of these notifications. Firstly there was the issue of bank accounts being set up incorrectly and secondly the issue of a change of address being notified to the financial institution, but not processed correctly. When these issues are treated separately from the general postal breach category, it brings the number of postal breaches down from 1,142 to 667. (See figure 2)

**Figure 2 – Breaches by Category – breakdown of postal breaches**




Measures which were put in place to address the issue of postal breaches in Allied Irish Banks are described in Case Study 16 in Part II of this Report.

Part II of the Report also includes three further case studies – one involving a major retailer and discarded credit card slips, one involving a missing backup media tape in O2 and one involving the disclosure of patient data to an incorrect fax number by the Health Service Executive.

## Privacy audits

The Commissioner is empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Scheduled audits are intended to assist the data controller in ensuring that their data protection systems are effective and comprehensive and are sometimes supplementary to investigations

carried out by the Office in response to specific complaints. Priorities and targets for audit are identified taking account of complaints and enquiries to the Office. During 2012, we continued to adopt a proactive role in this regard. The Office also continued with its programme of unscheduled inspections under powers conferred under section 24 of the Data Protection Acts.

Similar to the strategy adopted in 2011, we chose to tailor the programme of audits to allow us to focus on a few carefully selected targets and analyse them in intensive detail: namely An Garda Síochána; Facebook Ireland by way of a follow-up audit; and the conclusion of the investigation into INFOSYS.

**Organisations audited in 2012:**

In the course of 2012, 40 audits and inspections were carried out by this Office. This is an increase on the previous year – 2011 - in which 33 audits were completed in total. Included in the list of the audits/inspections, is the INFOSYS investigation which, although initially a 'desk audit', eventually led to a large number of meetings and visits to agencies within the public sector who had access to INFOSYS.

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

**List of Organisations audited/inspected**

O2
Anotherfriend.com
Irish Cancer Society
De La Salle College, Waterford (issue specific)
An Garda Síochána
Facebook-Ireland (follow-up review)
MedServ

Cork Co Council - Infosys
Dun Laoghaire Rathdown CC - Infosys
HSE Dublin Mid Leinster, Cherry Orchard - Infosys
HSE Dublin Mid Leinster, Naas - Infosys
Dublin City Council - Infosys
HSE South Kilkenny - Infosys

Ulster Bank (reporting procedures with the Irish Credit Bureau)
Permanent TSB (reporting procedures with the Irish Credit Bureau)
National Irish Bank (reporting procedures with the Irish Credit Bureau)
Bank of Ireland (reporting procedures with the Irish Credit Bureau)
St Raphael's Garda Credit Union (reporting procedures with the Irish Credit Bureau)
Waterford Credit Union (reporting procedures with the Irish Credit Bureau)

Cowper Care Centre Ltd - Glebe House Nursing Home, Kilternan, Dublin 18 (issue specific)
Dublin Coach (issue specific)
BOI Cabinteely (issue specific)
Trinity College (issue specific)
Permanent TSB (Open 24) Blackrock (issue specific)

Dublin Castle (OPW) (issue specific)

The Red Door School, Monkstown, Co. Dublin (issue specific)
The Criminal Courts of Justice (CCJ) (issue specific)
Spar, Finglas (issue specific)
Largo Foods Ashbourne Co Meath (issue specific)
Certus, St. Stephen's Green (issue specific)
Irish Bank Resolution Corporation, St. Stephen's Green (issue specific)
Dublin Bus, Phibsboro (issue specific)
Department of Arts Heritage and the Gaeltacht (issue specific)
Soho Bar, Grand Parade, Cork (issue specific)
OIS Services, Carrigaline, Co. Cork (issue specific)
Electric Ireland (issue specific)

Injuriesboardireland.com (desk audit)
National-accident-helpline.ie (desk audit)
Injury-Compensation- Ireland (desk audit)
Personal Injury Line (desk audit)

***An Garda Síochána***

An audit of An Garda Síochána (AGS) (national police force) commenced in 2012. As the audit entailed the examination of a wide range of issues relating to data protection, the initial stages of the audit programme were focused on obtaining an overview of the various kinds of personal data processed within An Garda Síochána.

The scope of the audit was acknowledged in advance by both parties as vast in terms of the datasets maintained by AGS. In view of this, it was agreed to refine and identify particular areas for examination such as the recording of incidents and crimes on PULSE (An Garda Síochána's primary computer system), inappropriate access to PULSE by members of AGS and also to examine specific areas administered by AGS such as the Garda Information Service centre in Castlebar, CCTV and Garda vetting. The audit focused on PULSE - a system onto which data regarding all individuals who come to the attention of the Gardaí are entered.

The chief finding was the discovery of inappropriate access to PULSE by An Garda Síochána during the course of the audit itself. We ran an ad-hoc on the spot inspection of usage and access to PULSE in relation to a substantial number of public figures or celebrities who were recorded as 'victims' or 'witnesses' on PULSE. Due to the excellent inbuilt trail functionality in PULSE, it was immediately apparent that two high-profile figures had their records accessed over 80 and 50 times respectively by members of AGS. In addition, the number of PULSE accesses returned on the records of three high profile media personalities and also a well known inter-county GAA player appeared to bear no relation to the valid entries relating to these individuals in connection with official police business. In all cases, there was no commonality in the members who had looked up these individuals. This was raised as a matter of urgency immediately with senior management in AGS and we were informed that the system of audit and review of user access which had been discussed extensively with this Office during its development was in place and was awaiting implementation. The new review system places a responsibility on District Superintendents to require members to account for the business reason for a specified percentage of accesses to the system per month. These accesses are chosen at random by the review system and provided to the Superintendent in each case. AGS confirmed that the conduct of the review will be a performance requirement of each Superintendent with failure to do so leading to action. Additionally, as part of the new audit structure of Garda access to PULSE, AGS stated that it intended that six districts out of a total of 137 districts would be audited per month by the Professional Standards Unit in AGS on a rolling basis.

In partial response to the finding of inappropriate access, (in any case a circular on the subject was already drafted and was referred to by AGS in advance of the audit), the Commissioner of An Garda Síochána issued a HQ Circular to all members of the Force on 06 December 2012 which inter alia stated "it is essential when enquiries are carried out on Items of Interest i.e. Persons Vehicles Locations, full information should be included in the "reason" for enquiry field in accordance with instructions at Code 32.15(3) and HQ Directive 14/2001. There will be no exceptions to this."

We intend to follow-up and to examine evidence of the new audit review programme.

***Facebook-Ireland Follow-up Report***

In 2011, a major audit of Facebook Ireland (FB-I) was conducted, the report of which was published in December 2011. Arising from the audit, FB-I agreed to a wide range of "best practice" improvements with a formal review of progress to take place in July 2012.

In September 2012, the Office published the outcome of our review of Facebook Ireland's (FB-I) implementation of recommendations made in our Audit.

The Review found that the great majority of the recommendations were fully implemented to our satisfaction, particularly in the following areas:

- The provision of better transparency for the user in how their data is handled,
- The provision of increased user control over settings,
- The implementation of clear retention periods for the deletion of personal data or an enhanced ability for the user to delete items,
- The enhancement of the user's right to have ready access to their personal data and the capacity of FB-I to ensure rigorous assessment of compliance with Irish and EU data protection requirements.

Those recommendations which were not implemented by FB-I as of that time were highlighted with a clear timescale for implementation listed. A deadline of 4 weeks for those matters to be brought to a satisfactory conclusion was set and FB-I progressed those matters to our satisfaction within the four week period. The Office

continues to maintain an ongoing dialogue with FB-I on the data protection implications of all new services as these are rolled-out.

Throughout the year the Office consulted extensively with colleagues in other Data Protection Authorities on matters which were arising in the context of the Audit process and matters that were of concern or interest to colleagues more generally. In so far as possible we sought to take these issues on board and to achieve satisfactory outcomes. This arose from our recognition that, while we had lead responsibility for the supervision of Facebook in Europe via its Irish establishment, that it was necessary to fully consult with and take account of the views of colleagues whose citizens had concerns about aspects of Facebook's use of their personal data.

***INFOSYS***

INFOSYS is a social welfare database administered by the Department of Social Protection. The INFOSYS investigation focused on the authorised use of INFOSYS by a whole range of external third parties, including local authorities, the HSE and other state agencies. The report of our investigation is published in full as an appendix (appendix 4) to this report.

We wish to particularly commend the Department of Social Protection on the monitoring systems it has in place for identifying any staff member inappropriately accessing records held by it. The Department has a clear focus on the protection of its customers' personal data. Unfortunately, as the findings in the report outline, the external agencies provided with access to INFOSYS did not always demonstrate the same good practices.

## Policy issues

***Household Charge***

Following the enactment of the Local Government (Household Charge) Act 2011, some public concern arose in relation to the extent and implications of the provisions contained in that Act for the seeking and sharing of personal data in order to identify properties liable to the charge. Following the enactment of the legislation, we had

already raised concerns with the Department of the Environment & Local Government in relation to the operation of the data sharing provisions in the legislation. The Department responded to those concerns and agreed to the development of a data sharing protocol with the Office that would address the circumstances in which data would be sought by the Local Government Management Agency; the data that would be sought; the immediate deletion of data once it was used; and the security conditions under which it would be transmitted and stored. The Protocol was published on the household charge website on 27 April 2012. The substance of the Protocol was reflected in the Local Property Tax Bill, 2012, which provides for a property tax to replace the household charge.

***Data Protection Guidance for primary and secondary schools prepared by School Management Bodies***

During 2012, we were approached by a working group of representatives from School Management Bodies to review draft data protection guidance for primary and secondary schools. We met with the working group and also reviewed two draft versions of the guidelines. This initiative by school management bodies to produce comprehensive data protection guidance specific to schools and how they process both personal and sensitive personal data is very much welcomed. Schools themselves have been the source of a large amount of queries to this Office in relation to their data protection responsibilities. The finalisation and dissemination of these guidelines, hopefully during 2013, will facilitate a better understanding of the requirements of the Acts as they apply to both primary and secondary schools.

***Credit Reporting Bill***

In September, the Minister for Finance published the Credit Reporting Bill 2012. The Bill provides for the establishment and operation of a statutory Central Credit Register (CCR) system in Ireland.

The Bill provides for the establishment of a mandatory credit reporting and credit checking system. It is intended that this system will be regulated and operated by the Central Bank of Ireland, its objective being to ensure that lenders have access to the most accurate and up to date information regarding a borrower's ability to repay.

During 2011, the Office participated in an Inter-Agency Group on Credit Histories established by the Department of Finance. The Credit Reporting Bill is based on the report which the Working Group produced. Given the role envisaged for this Office in the draft legislation, we closely engaged with the Department of Finance in relation to the drafting of the legislation itself.

We will continue to engage with the Department and other relevant stakeholders in relation to this draft legislation and its implementation, when finalised, to ensure that data protection considerations are satisfactorily addressed.

***Investigation in relation to inaccurate records held by the Irish Credit Bureau***

In May of 2012, the Office was contacted by Allied Irish Banks (AIB) concerning a serious data security breach relating to the data it passes on to the Irish Credit Bureau (ICB) in respect of the repayment history of some of their customers.

By way of background information, the ICB is an electronic library or database that contains information on the performance of credit agreements between financial institutions e.g. banks, credit unions and borrowers (i.e. the citizen). ICB is owned and financed by its members which are mainly financial institutions and over 140 lending institutions register information with the ICB, usually on a monthly basis. Each time an individual applies for credit from one of these lenders, the lender accesses that individual's credit report to find out about their performance under previous credit agreements with other lenders. Information is held for five years after a credit agreement is closed. It is normal practice that an individual provides consent for such a credit check to be carried out as part of an application for credit. An individual can, at any time, apply for a copy of their credit report from the ICB.

A key principle of data protection is the right to have personal information kept accurate and up to date. The ICB is wholly reliant on the accuracy of the data transmitted to it by its members and this subsequently forms the basis for an individual's credit report. The ICB do not decide who should get credit, but an individual's ICB report is an important factor in a financial institution deciding whether or not to award credit. Having regard to the volumes of personal data held by the ICB, this Office receives relatively few complaints regarding the accuracy of data held by it. However, in all such complaints, the issue can only be resolved by this Office clarifying the position with the financial institution concerned rather than with the ICB, and by the subsequent transmission of the corrected data concerned, where appropriate, from the financial institution to the ICB.

In the particular incident reported to this Office by AIB, it transpired that, for the previous 6 years, AIB had been supplying incorrect data to the ICB in relation to a number of its customers. Where customers paid loans on a weekly or fortnightly basis, AIB was reporting these repayments as if it were a monthly repayment. Therefore, if a customer missed 1 or 2 weeks on a repayment, this was being recorded with the ICB as 1 or 2 months where repayments were not made. This could have had a negative impact on the customer if they applied for credit and an ICB check was carried out by another lender. Following detailed discussions with this Office, the matter was resolved by AIB writing to the potentially impacted customers (circa 12,000) informing them of the error and ensuring that all historical customer payment records currently held at the ICB had been corrected. In addition AIB put in place system changes to prevent a recurrence of this issue. AIB also offered to request a copy of the customer's ICB statement from the ICB at its expense.

Following on from the reporting of this data protection breach by AIB, we undertook to conduct a series of inspections of financial institutions to examine all aspects of their reporting to the ICB. A cross-sectoral approach was adopted in order to identify inconsistencies in reporting practices that needed to be addressed. This matter was prioritised within the Office due to the harm that can result for an individual from the reporting of inaccurate information to the ICB. Four banks and two credit unions were selected for inspection and they were informed that the inspection would focus on all aspects of their reporting to the ICB. One of the principal outcomes of these

inspections was that we noted that there is now an individual/section tasked with overall responsibility for reporting to the ICB. However, it was acknowledged that, in the main, this was relatively new and that in some instances the AIB issue had served as a wake up call to financial institutions as to the importance of their responsibilities in regard to the ICB reporting process. Due to the previous lack of overall responsibility in this area, the team discovered that, in two of the banks inspected, up to very recently, there were entirely separate processes for managing ICB reporting within the institution itself.

The ICB issues monthly reports to financial institutions concerning what they consider may be inconsistencies in their ICB reporting, such as what happened in AIB where the arrears profile may not have been in a linear sequence. However, in one of the banks audited, it transpired that, while the Mortgage Unit had a systematic approach to dealing with such reports by checking each of the accounts concerned, the other lending arms of the bank did not. The bank concerned had informed this Office, prior to the inspection, that it had an issue with the misreporting of loans with a weekly/fortnightly repayment profile, similar to that which happened in AIB.
It was acknowledged that, had the processes in place in the Mortgage Unit for checking monthly reports from the ICB been in places across all the bank's credit portfolios, this issue would not have arisen. Similarly, it was discovered that, while one lending area in one of the banks audited had comprehensive processes for dealing with ICB error reports, the other lending areas in that bank had no such defined processes. Our view on this is that, if there is no defined uniform process in place in a financial institution to review monthly reports received from the ICB, this can potentially lead to the failure of identifying any emerging systemic ICB reporting issues. However, it is certainly anticipated that the new roles and responsibilities in this area will greatly improve this issue.

The team discussed with the various institutions how they reported loans which have been restructured and again considered that practices in relation to reporting of such agreements varied across the financial institutions inspected. The ICB manual provides financial institutions with a range of alphabetic profile indicators which can follow payment profile indicators 0,1,2,3,4 etc. The Code "M" is defined as "Moratorium- Lender and borrower agree to suspend all or part of the payment for

this period". In two banks inspected the team was informed that the code "M" is used only in cases of an agreed payment break i.e. the bank had agreed to suspend all payments, both capital and interest, for a defined period of time. In all cases where a mortgage has been restructured and where payments are being made in accordance with the restructuring agreements, these were being reported in the normal way i.e. 0, 0,0, 0,0,0. However, this was not the case in the two other banks where the position was that, where a customer entered into a forbearance /restructuring agreement with reduced capital and/or interest repayments, these were being reported as "M" i.e. Moratorium to the ICB. The Office expects that consistency in the reporting of repayment arrangements such as those outlined above will be clarified as part of changes to the credit reporting system envisaged in the Credit Reporting Bill 2012.

Another aspect of these inspections was the information supplied to customers as to how any alternative repayment arrangement will be reported to the ICB and the impact of this on the borrower's credit rating, in line with Paragraph 37 of the Code of Conduct on Mortgage Arrears issued by the Central Bank in 2010 which states, among other things, that where an alternative repayment arrangement is offered by a lender, the lender must provide the ***borrower*** with a clear explanation, in writing, of the alternative repayment arrangement, including how the alternative repayment arrangement will be reported by the lender to the Irish Credit Bureau and the impact of this on the ***borrower***'s credit rating. This is in line with the data protection principle, to have personal information obtained and processed fairly. In general, the team was satisfied that this provision was being complied across the financial institutions inspected. A sample of the wording being supplied to the customer included "I/We acknowledge that the taking of any Capital Payment Holiday will appear on the records of the Irish Credit Bureau (or other credit reference agency or agencies which the bank may use) and my/our ability to borrow in the future may be affected accordingly".

The team also questioned the various financial institutions on their processes for handling customer complaints as such complaints can be a vital component identifying any systemic issues which may be affecting the accuracy of reporting to the ICB and again it was considered that appropriate complaints handling procedures were now in place across the financial institutions inspected.

Overall the inspection team considered that there was good awareness across the financial institutions inspected of the importance of ICB reporting. We consider that the incident in AIB which gave rise to this issue in the first instance served to highlight to financial institutions as well as the general public the importance of the accuracy of ICB reporting.

## EU & International Responsibilities

***New EU Data Protection Laws***

In January the European Commission published its proposals[5] for a strengthening of EU data protection law, reflecting the enhanced status given to data protection by the Lisbon Treaty. The Commission proposals provide for a directly-applicable Regulation imposing stricter obligations on data controllers and processors and enhanced rights for data subjects. The Commission proposes a separate Directive covering the area of criminal justice.

The proposals have been the subject of much discussion in the course of the year, particularly by the co-legislators, the European Parliament and the Council of Ministers. The Minister for Justice, Equality and Defence invited submissions on the proposals in March. The Article 29 Working Party issued two Opinions[6] on the proposals.

It was expected that an effort would be made in the first half of 2013 – during the Irish Presidency of the Council – to reach broad agreement on the proposals.

The proposals, if passed into law, will involve increased responsibilities for our Office under the so-called "one-stop-shop" arrangement for multinational companies

[5] http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
[6] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_en.pdf
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf

providing services to EU users from an Irish base. While the exact division of labour between data protection authorities has yet to be finalised, it clearly will involve a greater degree of responsibility for our Office in relation to multinational companies which choose Ireland as an EU base.

### *Article 29 Working Party*

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

In the course of 2012, the Working Party continued to give close attention to issues relevant to the future EU data protection regime. It produced Opinions on the data protection reform proposals; cloud computing; biometrics; international data transfers; and "cookies".

The Working Party also gave its views on various other issues under consideration by European institutions or of relevance to its general data protection advisory role.

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

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

### *Data Protection in EU Specialised Bodies*

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

***International Activities***

We were represented and spoke by invitation at the 33rd[d] International Conference of Data Protection and Privacy Commissioners hosted by our colleagues in Uruguay and the European Conference hosted by our colleagues in Luxemburg.

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

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

Accountability of organisations for the personal data processed under their control is a key underlying concept in data protection law and practice. It is reflected in various articles of the draft revised data protection laws put forward by the European Commission. The renewed focus on accountability has been greatly facilitated by a project led by the US-based Centre for Information Policy Leadership. The project has been exploring what an organisation needs to do to demonstrate that it can be trusted to handle personal data. We have been participating in the project from its inception. A key output from the project in 2012 was a self-assessment tool designed to facilitate the internal review of an organisation's privacy and data protection programmes and practices.

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

# Administration

***Running Costs***

The costs of running the Office in 2012 were as follows:

| | **2012 €** |
|---|---|
| Overall running costs | **1,552,468** |
| Receipts | **647,721** |

A fuller account of income and expenditure in 2012 is provided in Appendix 3.

## Part 2

CASE STUDIES

***Case Study 1: Insurance Companies Prosecuted for Registration Offences***

In February 2012 three insurances companies, Zurich Insurance Plc, FBD Insurance Plc and Travelers Insurance Company Limited appeared in the Dublin District Court on charges relating to the processing of personal data by them in contravention of Section 19 of the Data Protection Acts.

**Background**

A formal data breach report was received by the Office in December 2010 from the Department of Social Protection concerning the alleged leaking to third parties by one of its officials of personal data held on the Department's computer systems. We immediately launched an investigation which identified two suspect entities engaged in ongoing contact with the official in question. Having established the identity of these entities we carried out an unannounced inspection at a firm of private investigators, Reliance Investigation Services Ltd, in Co. Kildare. During the course of that inspection, we obtained a copy of that firm's active client list for 2010. Having examined the client list, we identified that Zurich Insurance Plc, FBD Insurance Plc and Travelers Insurance Company Ltd were active clients of the private investigator. To progress the investigation of the data breach, the Commissioner requested Authorised Officers to conduct inspections at all three insurance companies. These inspections took place in December 2010.

Using the information which had been obtained at the premises of the private investigator, a number of claim files were identified in each insurance company as cases in respect of which the private investigator had provided services to insurance companies concerned. The email systems and a number of files were examined in both manual and computer form during the course of those inspections. Over the course of the following months, we continued our investigations by examining this information and during this time also received from the Department of Social Protection a list of all of the computer accesses made in 2010 on the Department's computer systems by the official suspected of committing the data breach. This led to the identification of further cases which required examination in the context of the investigation of the data breach. Further inspections took place at all three insurance companies in 2011. During these inspections, our Authorised Officers identified a

number of cases which were of interest in the context of the data breach investigation. Amongst some of those cases were reports submitted by the private investigator which contained information of a social welfare nature. The Authorised Officers sought and were provided with copies of private investigator reports in respect of several cases of the five individuals. The information which appeared to us to contain social welfare data of the individuals concerned was presented by us to the Department of Social Protection in August 2011 for examination. We subsequently received written confirmation from the Department of Social Protection in respect of each of the individuals concerned that the Department's computer system contained a data set of information relating to the individuals, that the data was used by the Department for the performance of its functions, that the data was "social welfare data," that the information on the sheets matched the social welfare data stored on the Department's computer system and that the social welfare data concerned was stored securely on the Department's computer systems and was not publicly accessible.

**Register Entry**

Under Section 16 of the Data Protection Acts, the Data Protection Commissioner has established, as is required, a public register of data controllers and data processors who are obliged to apply to be registered and to give certain details about their processing of personal information. Insurance undertakings fall into the category of data controllers which are required to be registered. All three insurance companies had current entries on the register at the time of this investigation. We examined all the register entries for each company. We noted that a description of personal data in the form of social welfare data was not recorded on the register entry. We also noted that the purpose for which personal data in the form of social welfare data was processed by the insurance companies was not recorded on the register entry. Having examined the data breach investigation file and the register entries for each of the three insurance companies, the Commissioner decided to initiate prosecution proceedings for breaches of section 19 of the Data Protection Acts. This section sets out the effect of registration. It provides, among other things, that a registered data controller shall not keep personal data of any description other than that specified in the register entry and that the data controller shall not keep or use personal data for a purpose other than the purpose described in the entry.

**Court Hearing**

On 13 February, 2012 the Dublin District Court accepted jurisdiction in the matter. Each of the defendant insurance companies pleaded guilty to ten charges in respect of breaches of Sections 19(2)(a) and 19(2)(b) of the Data Protection Acts. Having heard the prosecution evidence, the Court was satisfied that the prosecution case had been proven. Section 1(1) of the Probation of Offenders Act was applied in the case of each defendant company. Each of the defendant companies made an offer of a charitable donation of €20,000 to be paid to a charity of the Court's choosing. In each case, the Court accepted the offer and it directed that all three payments be made to the Capuchin Day Centre within two weeks. The Office also recovered from the defendants the legal costs arising from the prosecution.

**Other Matters Arising**

The Department of Social Protection also notified An Garda Síochána of the data breach and separate Garda investigations have taken place focussing on the source of the leakage and the role of private investigators in the breach.

***Case Study 2:<u>Unacceptable delay by O2 in processing an access request</u>***

We received a complaint in March 2012 in relation to the alleged failure of O2 (a Telecommunications company) to comply with an access request made to it in January 2012 seeking a copy of call records in respect of a mobile phone number from November 1999 to the date of the access request. In response to an access request, a data controller must supply the personal data to the individual within forty days of receiving the request.

We commenced our investigation initially by way of telephone contact with O2 during which we were assured by the company that it would immediately contact the requester's legal representatives to progress the matter of the access request. O2 subsequently wrote to the requester's legal representatives requesting a fee of €6.35 for the processing of the access request. It also informed them of the two year retention period applying to such data as set out in the Communications (Retention of Data) Act, 2011 and it informed them that call records beyond two years were not available.

The requester rejected the suggestion that there were limitations on the availability of call records beyond two years. They were informed by O2 that it was not simply a technical limitation but a legislative limitation and obligation incumbent on it on foot of the Communications (Retention of Data) Act, 2011 which obliges telecommunications service providers not to retain any such call data after a period of two years has elapsed.

In April 2012 O2 provided us with a copy of a letter which it sent to the requester's legal representatives informing them, among other things, that the mobile number for which the data was requested was an unregistered number. We urged the requester's legal representatives to provide O2 with any information available to substantiate ownership of the mobile number.

During the course of a subsequent conference call with O2 we established that the telephone number used by O2 when conducting its initial search of its database contained an incorrect digit. A further search by O2 using the correct digit established

that the phone number was registered to the requester. We instructed O2 to commence the process of retrieving the call records immediately.

O2 informed us in August 2012 that the retrieval process had been completed and that a copy of the call records for the previous two years had been provided to the requester's legal representatives in response to the access request.

The requester's legal representatives subsequently requested a formal decision under Section 10 of the Data Protection Acts. The Commissioner found in his decision that O2 contravened Section 4(1)(a) of the Data Protection Acts by not providing the relevant personal data within the time limit specified in respect of the access request submitted to it in January 2012.

There were several failings on the part of O2 in the processing of this access request:

- The Data Protection Acts provide at Section 4(1)(c)(i) that a fee may be payable to the data controller in respect of an access request. O2 requested the fee of €6.35 more than two months after the receipt of the access request and it did not commence processing the request until the fee was received. As the application of the fee is entirely discretionary on the part of the data controller, it is our view that if the data subject does not submit the fee with the access request, the onus lies on the data controller who intends to apply the fee to request payment at the earliest possible opportunity within the forty day statutory period. In the meantime, the data controller should continue to process the access request with a view to meeting the forty day timeframe for release of a copy of the personal data, subject to the fee being received within that timeframe. If the fee is not submitted until after the statutory timeframe, the data controller is not obliged to release a copy of the data sought until it receives it. However, a data controller may not delay the processing of a data access request and the release of a copy of personal data by failing to request payment of the fee until the statutory timeframe of forty days has either elapsed or is about to elapse within a few days.

- The data retrieval process did not commence until the end of May 2012, four months after the receipt of the access request. This was due to O2's delay in

requesting the fee and the fact that its initial search for records was conducted using an incorrect number. As a result of these delays, four months of data which the data subject wished to access was no longer in existence by the time the data retrieval process commenced.

- The data retrieval process was completed in August 2012. By O2's own admission and due to technical limitations all such requests made to O2 can take up to ten weeks to process. Therefore, had the retrieval process commenced as soon as the access request was received, the 40 day statutory timeframe in which such requests must be complied with would still have been exceeded - thereby resulting in a breach of Section 4(1)(a) of the Acts.

***Case study 3: <u>Access Restriction Under Section 5(1)(a) Requires A Prejudice Test</u>***

We received a complaint from an individual in relation to an access request he submitted to the Health Information and Quality Authority (the Authority). The complainant had worked as a healthcare assistant in a nursing home and was allegedly involved in an incident there. Details of this alleged incident were reported to the Authority and the individual concerned sought to access any personal information now held by the Authority.

The Authority refused to provide the requester with a copy of the personal data held by it as it was of the opinion that the data was exempt from disclosure under Section 5(1)(a) of the Data Protection Acts 1988 and 2003. This provision states that Section 4 of the Act does not apply to personal data *"kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders …. in any case in which the application of that section to the data would be likely to prejudice any of the matters aforesaid."* The Authority stated that the data it held in relation to the requester was kept for the purpose of preventing, detecting or investigating offences under Section 79 of the Health Act 2007.

We commenced an investigation by contacting the Authority, we informed it of the nature of the complaint and we requested that it explain how it had come to the view that the requester's personal data in this case was exempt from disclosure under Section 5(1)(a). It was not immediately clear to us that personal data relating to an alleged incident involving a healthcare assistant came within the ambit of the offences which the Authority had power to investigate and/or prosecute.

The Authority stated that the offences within Section 79(2) of the Health Act 2007 related *inter alia* to compliance by the registered provider (i.e. the nursing home) with the Health Act 2007 (Care and Welfare of Residents in Designated Centres for Older People) Regulations 2009. It said that the offences thereunder are offences to which the registered provider would be subject to sanction and, for that reason, it was considered that the data fell under the ambit of Section 5(1)(a). Regarding the status of the investigation into alleged offences under the Health Act 2007 we were informed that following its initial review the matter was concluded from a care and

welfare perspective. However, the Authority indicated that it intended to keep the file on the matter active until the relevant statute of limitations period has elapsed.

We advised the Authority that a prejudice test applied to the applicability of the exemption under Section 5(1)(a). We also pointed out that the requester's right to access personal data is confined to that data which relates to them, or by which they can be identified. We pointed out that this does not provide a basis for the requester to access from a report or files information which is not their personal data. We informed the Authority that while it was a matter for it to determine in the first instance, it was not immediately obvious to us what prejudice would arise in relation to an investigation by releasing the personal data to the requester in this case.

The relevant issue for the Authority to consider was whether the provision of the requester's personal data would be likely to prejudice the Authority's ability to investigate the alleged non-compliance by the care home with the Health Act 2007. Following a further examination, the Authority concluded that no prejudice would arise by the release of the personal data concerned. The requester was subsequently provided with a copy of the personal data concerned.

While the Data Protection Acts restrict the right of access to personal data where that data is kept for the purpose of investigating and/or prosecuting offences, the mere existence of such an investigation or proceedings does not permit the exercising of a blanket exemption by the data controller across all personal data held by it. The personal data of an individual who requests access to such data may only be withheld where the provision of that data would be likely to prejudice the particular investigation or prosecution proceedings. The exemption is not a permanent one. Where investigations and follow-on proceedings (if any) have been completed it is unlikely that those matters can continue to be prejudiced by the release of the personal data concerned. Once the prejudice no longer exists, the exemption used to withhold the personal data ceases to apply and a copy of the personal data must be made available to the data subject.

***Case study 4: <u>Discovery Process Reveals Data Protection Breach.</u>***

We received a complaint in September 2011 from an individual in relation to the alleged failure of the Dublin Airport Authority to comply in full with an access request made to it in May 2005. Dublin Airport Authority had responded to this access request in July 2005 stating that it held no personal data in relation to the requester. Some years later, however, a number of documents were produced following a discovery process undertaken by the Dublin Airport Authority pursuant to High Court proceedings. In that context, the data subject was given access to a copy of three documents which contained some personal data relating to him. These documents pre-dated the access request made in 2005. The data subject complained that his right of access had been wrongly denied six years previously.

Having examined the documents concerned, we were satisfied that they did contain some personal data relating to the data subject and that those items of personal data did fall due for release at the time of the access request in 2005. We commenced an investigation by contacting the Dublin Airport Authority on the matter and we sought a full explanation in relation to the handling of the access request in 2005.

We received correspondence from Dublin Airport Authority's legal representatives informing us that, following receipt of the access request in May 2005, Dublin Airport Authority identified a small number of documents in its possession relating to the request. They informed us that, at the time of the access request, an assessment of the documents was made in conjunction with legal advice obtained by the Dublin Airport Authority. This concluded that the documents did not constitute personal data within the meaning of the Data Protection Acts given that only passing reference was made to the data subject and that the data subject was not the focus of the documents in question. Consequently, a letter issued to the requester in July 2005 stating that Dublin Airport Authority held no data in relation to him which would be regarded as personal data.

The complainant sought a decision on his complaint. The Commissioner subsequently issued a formal decision which found that Dublin Airport Authority contravened Section 4(1)(a) of the Data Protection Acts, 1988 and 2003 by not providing the relevant personal data to the data subject within the time limit specified in respect of

the access request made in May 2005. The Commissioner specifically identified on the documents involved the text which he considered to constitute personal data of the data subject concerned. (The documents discovered on foot of the High Court proceedings contained non-personal information as well as some personal data relating to the data subject). As this case demonstrates, a court discovery process undertaken long after the access request was processed uncovered a data protection breach which took place at the time of the processing of the access request and this breach was caused by the data controller's interpretation of the definition of personal data. As a result, the data subject was wrongly denied his right of access to his personal data for a number of years.

***Case study 5: <u>High Court Rules That Personal Data Can Be Accessed By Litigant</u>***

My Office received a complaint in February 2010 from the legal representative of an individual concerning the alleged failure of Dublin Bus to supply her, in response to an access request, with a copy of CCTV footage of an incident involving her which occurred on one of its buses.

Córas Iompair Éireann Group Investigations Department responded to the access request stating that:

*"All documents and records in this office are prepared in contemplation of litigation. These days every incident is a potential claim and our files fall within legal professional privilege. In those circumstances, information in any form, is not disclosed pursuant to a Data Subject Access Request nor is our defence evidence disclosable. In the event of disputes on that point, you can apply to Court for a Discovery Order"*

The complainant also informed us that, at the invitation of Dublin Bus, the legal representative of the data subject had attended, on its client's behalf, at CIE Offices to view the footage concerned prior to the submission of the access request to the company.

**<u>Investigation</u>**

In commencing our investigation of the complaint we asked Dublin Bus to outline the specific circumstances under which the data subject's image was captured by CCTV systems operating in Dublin Bus and to provide an explanation as to why a copy of the CCTV footage was not provided to the data subject in response to her access request. We stated that it was unlikely that CCTV footage of an incident would fall under the legal professional privilege exemption provided for at Section 5(1)(g) of the Data Protection Acts.

Dublin Bus responded by claiming *"the CCTV footage was preserved solely for use in the defence of any litigation arising out of the accident and regardless of whether or not litigation is yet in being it is privileged."*

In attempting to progress our investigation we gave Dublin Bus a number of opportunities to re-consider its position on the application of the Section 5(1)(g) exemption. However, it maintained its position and it refused to supply a copy of the footage in response to the access request.

**Enforcement**

An Enforcement Notice was served on Dublin Bus in January 2011 requiring it to provide the data subject with a copy of the CCTV footage concerned. The Notice stated that the Commissioner was of the opinion that Dublin Bus was in contravention of Section 4(1) of the Acts in failing to comply with an access request made to it in February 2010. Dublin Bus appealed the Enforcement Notice to the Circuit Court. Subsequently, Dublin Bus requested that the Enforcement Notice be withdrawn as the data subject sought discovery in April 2011 in the context of High Court proceedings of all information held by Dublin Bus relating to the incident which had allegedly taken place on the bus. The Commissioner did not accede to this request.

**Circuit Court**

In its appeal to the Circuit Court in May 2011 and relying heavily on the UK *Durant* case, Dublin Bus submitted

- that the Enforcement Notice was an attempt to subvert the jurisdiction of the courts;
- that the CCTV footage did not constitute personal data within the meaning of the Data Protection Acts;
- that the CCTV footage was not held or maintained on a relevant filing system; and
- that the CCTV footage was downloaded solely for the purposes of the defence of anticipated litigation and is, as such, privileged.

Counsel for the Data Protection Commissioner submitted

- that the *Durant* case was irrelevant as the UK Data Protection Act 1998 gives the Court discretion as to whether to direct access to such data;

- that by allowing an inspection of the CCTV footage to the data subject's legal representatives, Dublin Bus thereby waived any privilege it claimed;
- that even if any privilege was not waived, Dublin Bus does not come within the exception provided at Section 5(1)(g) in relation to the CCTV footage in this case;
- that there is no provision in the Acts which precludes a data subject from exercising their right to access personal data to which they are entitled because they are litigating before the Court; and
- that there are no exemptions from the right of access where civil legal proceedings are contemplated or ongoing.

On 5 July, 2011 the Circuit Court judgment was delivered (Record No. 1316/2011). It ruled that:

- the CCTV footage concerned is personal data within the meaning of the Data Protection Acts;
- Dublin Bus does not come within the exception relating to privilege under Section 5(1)(g) of the Data Protection Acts from the obligation to comply with a data access request under Section 4;
- there are no exemptions under the Data Protection Acts from the right of access under Section 4 where civil legal proceedings are contemplated or ongoing; and
- the UK Data Protection Act 1998 is distinct from the Irish legislation in that it confers a discretion on the Court as to whether to grant an order for access.

The appeal by Dublin Bus was accordingly dismissed and costs were awarded to the Data Protection Commissioner.

**High Court**

Dublin Bus appealed the Circuit Court judgment to the High Court. The case was heard in June 2012 (Record No. 123CA/2011). Dublin Bus submitted:

- that the Circuit Court erred in law in holding that, subsequent to the commencement of legal proceedings, the High Court did not have the sole competence to deal with and adjudicate upon all of the matters arising between the parties relating to the accident;
- that the proper forum for adjudicating on matters of Discovery between the parties is the court which has seisin of the proceedings, in this instance, the High Court;
- that any attempt to seek disclosure outside of the High Court is a mistaken and inappropriate attempt to usurp the function of the High Court;
- that the role of the Data Protection Commissioner is protecting the data of the citizens of the state. The Commissioner should have no role in the conduct of litigation;
- that by affording an appellant the right to first appeal to the Circuit Court, and thereafter to the High Court on a point of law, the drafters of the legislation clearly intended that the Courts would have discretion in deciding upon the interpretation of the Acts. Therefore, the purposive effect of the Acts provisions must be considered, and it is on this basis that the dicta of *Auld LJ* in the *Durant* case retains very strong persuasive value in terms of the interpretation of the Irish Acts; and
- that the High Court should take cognisance of the dicta of *Auld LJ* that the purpose of data protection law is not *"to assist [a litigant].... to obtain discovery of documents that may assist him in litigation or complaints against third parties."*

Counsel for the Data Protection Commissioner submitted:

- that the Circuit Court was correct in its finding;
- that the serious and significant error test (in Ulster Bank v Financial Services Ombudsman [2006] IEHC 323) is of long standing in Irish law and is the appropriate standard to apply to this appeal;
- that a person's fundamental right to access their personal data under the Acts is not conditional upon their establishing a good motive for wanting their

personal data and the Commissioner is not required to demand of a requester why they want their personal data;

- that if the drafters of the legislation wished to impose limitations on the right of access to personal data in circumstances where litigation had been instituted they would have done so expressly;
- that there is nothing about making a data access request pursuant to the statutory right of access that amounts to subverting the jurisdiction of the courts, indeed quite the opposite, since the courts expect parties to see if they can obtain information from other sources before taking up the time of the court with a discovery request;
- that any exemption to data protection law should be narrowly construed since it is an exemption from a fundamental right.

On 8 August 2012 Hedigan J delivered judgment. He noted that no attempt had been made in the appellant's notice of appeal to identify any points of law. He stated "*From the Courts perspective this is completely unsatisfactory. Simply saying that you are appealing the whole of a judgment does not amount to a valid appeal on a point of law. An appeal on a point of law is just that. The point of law should be identified and the submissions should be directed to that point. When pressed on the matter, the appellant did identify the point of law which it wished to raise on appeal as follows: 'Whether the existence of legal proceedings between a data requester and a data controller precludes a data requester making an access request under the Act.'*"

Hedigan J found that the English case law relied upon by Dublin Bus was not relevant. He found that in effect the appellant was *"seeking to carve out a new exception in the Acts, to the effect that whenever a data requester has instituted litigation against a data controller he or she is precluded from making a data access request under the Acts."* Hedigan J accepted Counsel's submission that *"if the drafter of the legislation wished to place such limitations on the right of access to personal data then they would have done so expressly."*

Hedigan J concluded: *"Thus in my judgment, the existence of proceedings between a data requester and the data controller does not preclude the data requester making*

*an access request under the Act nor justifies the data controller in refusing the request. I am not therefore satisfied that the appellant has raised a point of law giving rise to grounds for overturning the decision of the learned circuit judge. I must therefore dismiss this appeal."*

The High Court subsequently made an Order for costs in favour of the Data Protection Commissioner.

The High Court's ruling in this matter is welcome as it provides important legal clarity on the right of access to personal data for individuals involved in matters of litigation while at the same time it defines for data controllers the narrow restriction to the right of access which is contemplated by the exemption in Section 5(1)(g).

***Case study 6: <u>Outstanding debt details legitimately passed on to debt collection agency</u>***

In January 2012, the Office received a complaint from an individual alleging that her personal data had been unfairly processed by the telecommunications company Hutchison 3G Ireland (Three). The complainant alleged that her personal data had been passed by Three to a debt collection agency without her consent.

The complainant informed us that she had entered into a twelve month broadband contract with Three and paid for the service by direct debit. She informed us that after the twelve months had expired, she cancelled her direct debit for payment of the service as she considered the contract was up. She stated that she also contacted Three to cancel her contract. The complainant alleged that she began to receive phone calls from Three querying the cancellation of her direct debit and in relation to an outstanding debt on her account. The complainant further informed us that, despite her communications with Three in relation to the matter, a number of months later she received a letter from a debt collection agency regarding her debt to Three.

This matter was raised with Three and in its response, it informed us that the complainant had originally signed up for a twelve month <u>minimum</u> term contract. It also informed us that all of Three's minimum term contracts remain in place following the expiry of the minimum term which is standard in the industry. According to Three, under the terms of its customer contracts, if a customer wishes to cancel a contract, they must provide thirty days written notice. In this case, Three informed us that the complainant continued to use the account long after the minimum term of twelve months had expired. Three further informed us that the complainant cancelled her direct debit payment for the broadband service prior to her cancellation of the contract and it sought to recoup the monies owed in respect of the broadband usage which occurred after the direct debit had been cancelled.

It also informed us that, in accordance with its normal debt collection process, it issued the account of the complainant to a debt collection agency. Three's terms and conditions clearly stated that it may use and share customer details for the collection

of any debts on an account and that this may include the use of debt collection agencies to collect debts on its behalf. In this case, Three used a debt collection agency to obtain repayment of the complainant's debt.

It was our view, following the investigation of this complaint, that Three did not unfairly process the complainant's personal data when it passed her details to a debt collection agency in order to have any outstanding debt collected.

This case study highlights that it is vital when individuals are signing up to contracts with any company, that they are fully aware of what they are signing up to. Terms and conditions of a contract should always be read and fully understood before committing to such a contract.

***Case study 7: <u>Collection of photographic identity by a fertility clinic</u>***

In November 2011 the Office received a complaint from an individual regarding what she considered excessive personal data being sought by a fertility clinic. The complainant informed us that she had been attending at the clinic, that she had been told at one of her appointments that the clinic required a photograph of her and her partner and that, without it, she could not proceed with the fertility treatment. The complainant allowed the clinic to take the photograph but she felt that it was excessive. The complainant alleged that she had not been informed at the initial consultation of the compulsory condition to provide a photograph. Following further communication with the clinic, the complainant was informed that the photograph was necessary to prevent and diminish any potential mistakes with identification of tissue tests and embryos.

We wrote to the clinic and we asked it to outline the basis for the collection of photographs, and the need for them to be retained on the clinic's database. We also asked if the same level of security could otherwise be achieved by having sight of the patient's photographic identification, without retaining a copy of it.

In its response, the clinic indicated that the basis for the collection of the photographs was to verify the identity of each patient when they presented for an appointment. It informed us that it believed this to be an appropriate security measure to minimise the risk of unauthorised access to or disclosure of medical records to anyone other than the presenting patient. It also informed us that it was not possible to maintain and provide the same level of security by having sight of photographic identity without retaining a copy.

As a result of this complaint, the clinic undertook to introduce some new procedures. This involves requesting all patients to sign a consent form for the taking of their photograph. If a patient refuses to sign the form, the data protection officer at the clinic will meet with the patient to explain the purpose of the photograph and to offer an alternative option of producing photographic identification at each appointment. In this case, the clinic undertook to facilitate the complainant and her partner's request to have their photographs removed from the database.

This Office was satisfied with the new procedures as they took into account the patient's preference while at the same time maintaining the same level of security which the clinic required.

***Case study 8: <u>Excessive use of CCTV in a Nursing Home</u>***

In April 2012, we received a complaint from an individual in relation to the operation of CCTV cameras at a nursing home. The nursing home had installed CCTV cameras in the corridors, day room, kitchen, front entrance, staff room, residents' dining room, games room and drug therapy room. Concerns were also raised that the CCTV system was linked to the owner's private residence allowing the cameras to be checked remotely during the night.

Images of people captured by CCTV cameras are personal data and the processing of such images is covered by the provisions of the Data Protection Acts. The use of CCTV cameras must be proportionate and transparent. We asked the nursing home to outline to us the circumstances under which CCTV footage was recorded and accessed. We also asked the nursing home to confirm if there was a linkage of the CCTV system to a private residence and its purpose.

In its reasoning for the use of CCTV, the nursing home informed us that it was to ensure the safety, protection and quality of care to its residents and also to ensure the safety and protection of staff. It also informed us that the CCTV system was not connected to a private residence but it was connected to the smart phones of both directors to allow them to maintain the quality and care of residents from a distance. It said that this alleviated the need for the directors to constantly make unannounced visits at night.

Having reviewed the nursing home's response we informed it that it was clear that it was using CCTV and live monitoring via cameras as a substitute for on-the-ground supervisory staff. We informed it that we could not see any basis under which the use of smart phones for live monitoring purposes could operate legitimately in accordance with the Data Protection Acts. We asked the nursing home to voluntarily cease the practice with immediate effect. We also asked it to provide some still screen shots taken from the CCTV cameras in the kitchen area so that we could consider further the appropriateness of the cameras operating in that area.

The nursing home immediately removed the CCTV camera from the staff room and it also disconnected the smart phone links to the CCTV system. It also provided screen shots from the CCTV cameras in the kitchen area. It explained that the kitchen area was unsupervised between the hours of 8pm and 8am and, as kitchens can be a dangerous place for elderly residents, it felt that the use of a CCTV camera was justified in this particular area.

Having fully reviewed the situation, we recommended that the camera in the kitchen be switched off during working hours when staff are present. We also gave the nursing home recommendations concerning changes we considered were necessary to the CCTV signage which was in place there.

Of particular interest in this case study is the concept of remote access to CCTV cameras. In this instance, the remote access was carried out by means of smart phones. Remote access to CCTV cameras, by whatever means, is becoming more frequent with advances in technology. Clearly such technology is helpful in terms of providing security monitoring of an empty building at night time or at weekends and no data protection issues arise in such situations. However, concerns from a data protection perspective arise where the remote access takes place in relation to areas such as manned workplaces and where workers perceive that their work performance is being monitored on a live basis. Employers are tempted to use such technologies as a substitute for on-the-ground supervision by supervisory or managerial staff. Such situations are difficult to reconcile with the requirements of the Data Protection Acts and this Office cannot see any legal basis to justify the monitoring of individuals in the course of their normal activities by such means. In instances such as that outlined in this case study, where there is no valid justification for the use of remote access technology to link to CCTV cameras, we will continue to order that the remote access concerned be terminated.

***Case Study 9: <u>Disclosure of Student Personal Data by Secondary School</u>***

In November 2011 we received a complaint from an individual concerning the alleged disclosure of his daughter's personal data by a secondary school at which she was a student, St. Joseph's College, Borrisoleigh, Co. Tipperary, to a third party. It was alleged that this disclosure took place by way of a letter issued by the secondary school to a third party without the knowledge or consent of either the complainant or his daughter.

By way of background, the complainant informed us that, following a complaint which he and his wife had made to the Board of Management of a local national school, he received correspondence from the Chairperson of that school's Board of Management in relation to that complaint. Included with that correspondence was a copy of a letter issued by St. Joseph's College which contained references to the complainant's daughter who was a student of that College. We were further informed that this letter, which was allegedly requested by a separate third party (a parent of a different student at St. Joseph's College) and addressed "To Whom It May Concern," was subsequently passed by that third party to the Chairperson of the Board of Management of the local national school.

My Office commenced the investigation of the complaint by writing to St. Joseph's College. We asked it for an explanation as to what led to the alleged disclosure and what steps were being taken to address the matter. We received a response from St. Joseph's College informing us that it would not be getting involved in our investigation at that juncture. We responded in early December 2011 stating that, as St. Joseph's College was the data controller in this instance, we required a response to our letter. In the absence of any further communication we issued a final warning letter to St. Joseph's College on 12 January, 2012 requiring it to respond to our investigation within fourteen days.

On the following day we received a phone call from the school manager of St. Joseph's College. He informed us that he did not have any knowledge of the issues between the complainant and his school. On the same phone call we then spoke to

the administrator of St. Joseph's College, the signatory of the letter in question. He informed us that when the third party requested the letter he (the administrator) did not know why he wanted it. He said that he was unaware that he breached the Data Protection Acts when he made references to the complainant's daughter in the letter. Later that day, we received an email from St. Joseph's College outlining the circumstances which led to the issuing of the letter to a parent of a student at the College and which referenced the complainant's daughter, a different student at the same College. In the email, the administrator indicated that the parent concerned did not state that the letter would be given to the Board of Management of a primary school. The College informed us that it had redrafted its data protection policy to ensure that the Data Protection Acts are fully complied with.

Having informed the complainant of the College's response to our investigation, we asked him if he was interested in seeking an amicable resolution of his complaint. In response, he indicated that he could not accept that there could be any informal resolution to his complaint and he sought a decision of the Commissioner.

In making the decision on this complaint, the Commissioner examined and considered all aspects of the case. He formed the opinion that St. Joseph's College contravened Section 2(1)(c)(ii) of the Data Protection Acts by disclosing the personal data of the student concerned to a third party without her knowledge or consent or the knowledge or consent of her parents. This contravention occurred when St. Joseph's College issued a letter in September 2011 containing personal data of one of its students under the heading "To Whom It May Concern" and gave it to a third party, namely a parent of a different student.

***Case Study 10: <u>Customer Data Transfer for Waste Collection Service in Dublin</u>***

In January 2012 the Office received several complaints and enquiries from citizens of the Dublin City Council area after they received a letter notifying them that Dublin City Council and Greyhound Recycling and Recovery had reached agreement on the sale of the Council's commercial and domestic waste collection business to Greyhound Recycling and Recovery. The letter indicated that Greyhound Recycling and Recovery would take over control of bin collections for the Council's 140,000 customers on 16 January, 2012 and that from that date the Council would officially transfer its waste collection business to Greyhound Recycling and Recovery. It went on to outline the annual service charge and lift fees which would apply to the service. It also gave details of the methods of payment and it included a customer payment card with a customer account number for the new Greyhound account. The letter also stated that the final City Council bill for the period ending on 13 January, 2012 would be issued and the revenue collected on behalf of the City Council by Greyhound Recycling and Recovery which would also collect any outstanding arrears on behalf of the City Council. Complainants to this Office expressed concerns in particular about the transfer of their personal data by Dublin City Council to a private company without their knowledge or consent.

We conducted a comprehensive investigation which focussed on both the transfer of customer data from Dublin City Council to Greyhound and the collection of Dublin City Council customer debts by Greyhound.

<u>The transfer of customer data from Dublin City Council to Greyhound.</u>

Our investigation concluded that the core elements of the sale of the business did not breach the Data Protection Acts. We established that the customer data transfer from Dublin City Council took place between 22 and 23 December, 2011. We noted that a notification letter regarding the new service provider was sent to customers of Dublin City Council in the first half of January 2012. The notification letter to customers should have taken place at a much earlier stage. By notifying customers of their new

service provider simultaneous to the completion of the sale but after the data transfer had occurred, it was not possible for the Office to come to the view that the "fair processing" requirements of the Data Protection Acts, 1988 & 2003 were fully met by Dublin City Council in this instance.

Dublin City Council agreed, in light of this experience, that in the event that any similar situation arises in the future, it will seek to comply with all relevant published Office of the Data Protection Commissioner guidance in relation to such matters in being at that time unless it obtains confirmation from this Office that compliance does not arise in a particular circumstance.

The collection of Dublin City Council customer debts by Greyhound.

Our investigation found that no transfer of personal data from Dublin City Council to Greyhound in respect of the collection of Dublin City Council customer debts had taken place. This was confirmed by the Office by way of an unannounced inspection at the premises of Greyhound and its agents on 26 January 2012. This inspection confirmed that only name, address and whether a household was entitled to a waiver were transferred to Greyhound.

We agreed with Dublin City Council and Greyhound that the customers of Dublin City Council and the customers of Greyhound must be assured that robust controls are in place at Greyhound to guard against any possibility of the cross pollination of debt collection information handled on behalf of Dublin City Council with personal data handled by Greyhound in the normal course of its waste collection activities. Accordingly, the following undertakings were agreed before any debt collection data was transferred from DCC:

- Staff at Greyhound or its agents who handle personal data in the context of debt collection for Dublin City Council will not have access to any personal data held in the context of Greyhound's waste collection business, and vice versa.

- The debt collection database held on behalf of Dublin City Council by Greyhound and/or its agent to be separate and distinct from all other aspects of Greyhound's waste collection business. All access and use of the personal data held on behalf of Dublin City Council to be auditable and verifiable via specific usernames and passwords.
- An audit procedure to be put in place by Dublin City Council to ensure that Greyhound, as a data processor on behalf of Dublin City Council, is fully compliant with all aspects of its data protection responsibilities as a data processor. An initial audit will take place within six months of the commencement of the debt collection function. The terms of the audit to be agreed with this Office. This audit will be conducted by a competent third party auditor to be agreed with this Office. Further audits will be scheduled on an annual basis (for so long as Greyhound are acting as a data processor on behalf of Dublin City Council in relation to customer debt collection in respect of outstanding waste collection charges). This Office will be supplied with a copy of each audit report.

This case serves to highlight the steps which must be followed and the considerations which must be given to the procedures which need to be put in place when customer data transfers are envisaged in the context of the sale or transfer of a business. A guidance note on "Transfer of ownership of a Business" is published on our website and we recommend that data controllers pay close attention to it in such circumstances.

***Case study 11: Department of Education Circular Leads to Complaint about Sick Leave Information***

We received a complaint relating to a Department of Education Circular (No. 0060/2010) concerning sick leave for registered teachers.

Specifically, the complaint focussed on certified sick leave and the requirement in the Circular that the nature of illness must be stated in a medical certificate in order for it to be acceptable.

Under the Data Protection Acts, medical data falls into the category of "sensitive personal data." An employer has a legitimate interest in knowing how long an employee is likely to be on sick leave absence from work. It also has a legitimate interest in knowing whether an employee, following an accident or illness, is capable of doing particular types of work. Requiring employees to produce standard medical certificates to cover absences due to illness does not therefore present any data protection issues. But an employer would not normally have a legitimate interest in knowing the precise nature of an illness and it would therefore be at risk of breaching the Data Protection Acts if it sought such information. Even the consent of the employee may not allow the disclosure of such information to an employer as there may be a doubt as to whether such consent could be considered to be freely given in an employment context.

The Office raised the matter with the Department of Education. The Department indicated that the purpose of such information was to ensure that there was sufficient information available to the employer to make an informed decision as to whether or not to make a referral to the Occupational Health Service and/or to take appropriate steps, where necessary, in relation to health and safety matters. It said that in the context of a school, where the employer has a duty of care to its students and staff and where a teacher often has sole and unsupervised access to, and responsibility for, children this was particularly important. It stated that in the Department's view, there was a strong legitimate public interest in ensuring that there was sufficient information to enable the employer to deal with any health and safety issues that may arise.

We accept that there are limited circumstances where employers may seek information from an employee in the context of an illness-related absence from work. Such situations may also permit a health professional to provide details of illness on request to an employer in specific circumstances where specifically warranted in a workplace context. Our guidance in relation to this matter (FAQ 3.7 on our website) makes it clear that in certain very specific circumstances a doctor may be legally obliged to report certain illnesses to an employer for health and safety reasons and we recognise the need for this practice, particularly in the case of contagious diseases. However, any general practice of requiring all employees to specifically disclose their condition or illness to account for their sick absences from work does give rise to serious concerns from a data protection perspective as it does not adequately protect the sensitive personal data of those employees who may have an illness/condition which they consider private or sensitive.

We indicated to the Department that all of the considerations it had outlined had been considered by a Working Group established by the Department of Finance in 2010, which included representation from various Government Departments, this Office and the Attorney General's Office. This led to the adoption of Department of Finance Circular 09/2010 setting out the Civil Service policy on the management of sick leave. In particular, Section 11 of that Circular states, among other things, that *"While the nature of the illness does not have to be included in all circumstances, if it is not stated this may give rise to difficulties if seeking to have the absence discounted."* We consider that this approach represents an appropriate balance between the concerns outlined by the Department and the legitimate privacy expectations of employees.

Following our intervention, the Department confirmed that it was no longer advising schools/teachers that the nature of illness must be stated in all cases where a medical certificate is required. The Department also undertook to reflect this change when revising the current sick leave circular for teachers in order to ensure compliance with the Data Protection Acts. In addition, the Department indicated that relevant staff had been notified of our findings on this matter.

This case study highlights that employers should be aware that, in general, only limited relevant information should be sought from an employee submitting a medical certificate to account for a period of sick absence. Seeking excessive sensitive personal data in that context is a clear breach of the Data Protection Acts.

***Case Study 12: Prosecutions - Unsolicited Marketing***

Advance Tyre Company Limited (trading as Advance Pitstop)

In June 2011, we received a complaint from an individual who received an unsolicited text message from Advance Pitstop in Dundrum. He informed us that he had never given his consent to receive marketing text messages from Advance Pitstop. We had previously sent a formal warning to Advance Pitstop in April 2011 informing it that, if we received any further complaints where offences were committed, we would prosecute it for those offences.

In this case, Advance Pitstop stated to us that it collected customer data via a form which customers were asked to complete in the branch. This included a tick box option for customers' marketing preferences. Advance Pitstop was unable to find in its records a form filled out by the complainant. The complainant also insisted that he did not fill out such a form. On this basis we decided to take prosecution proceedings against Advance Tyre Company t/a Advance Pitstop under Regulation 13 (1)(b) of SI 535 of 2003 (as amended) for the sending of an unsolicited marketing text message to an individual without consent.

On 11 June, 2012, at the Dublin District Court, Advance Tyre Company Limited pleaded guilty to the sending of an unsolicited text message to the complainant without consent. The Court accepted the guilty plea and it applied the Probation of Offenders Act on condition that Advance Tyre Company Limited pay €1,000 to a charity, the Laura Lynn Foundation. Advance Tyre Company also agreed to pay the prosecution costs incurred by the Office.

Ocsas Holdings Limited (T/A The Fitzgerald Group, etc)

At the same court sitting in the Dublin District Court, Ocsas Holdings Limited faced six charges arising from a complaint we received in July 2011 regarding unsolicited text messages and emails which the complainant received from the Fitzgerald Group. He informed us that he signed up to a loyalty card called "BeneFitz" in December 2010. At the time he said he ticked a box indicating that he did not wish to receive

any marketing communications from the company. Shortly afterwards, he began to receive both unsolicited marketing emails and text messages from the group. We had investigated a previous complaint regarding the Fitzgerald Group which resulted in a formal warning to it in February 2011.

The complainant emailed the Fitzgerald Group on two occasions asking to be removed from both the email and text message database of the Fitzgerald Group. He was informed by the Fitzgerald Group on both occasions in January and February 2011 that his details had been removed. However, the complainant then received further unsolicited marketing text messages in June and July 2011, prompting his complaint. It was clear to us that the Fitzgerald Group had not put proper procedures in place to ensure compliance with its obligations with regard to its marketing operations despite the previous warning. On this basis the Commissioner decided to prosecute the Fitzgerald Group under Regulation 13(1)(b) of SI 535 of 2003 (as amended) in relation to the sending of an unsolicited marketing text message to an individual without consent.

The Court accepted one guilty plea from Ocsas Holdings Limited T/A The Fitzgerald Group, etc. The Court ordered that it pay €1,000 to the Laura Lynn Foundation and it applied the Probation of Offenders Act. Our prosecutions costs were also recouped from the defendant.

Citywest Resort Limited

In early 2012, we received two complaints from individuals regarding unsolicited text messages sent by Citywest Resort Limited (trading as the Citywest Hotel, Conference, Leisure and Golf Resort) without consent and without the inclusion of an opt out option. All marketing emails promoted the Citywest Health and Leisure Club. Both complainants informed us that they had repeatedly contacted the Leisure Club requesting to be removed from the marketing database but they continued to receive further unsolicited marketing text messages. Previously, in August 2010, we had sent a formal warning to Citywest Health and Leisure Club with regard to its future marketing activities.

In response to our investigations, the Leisure Club admitted that it could not confirm that it had consent to send marketing text messages to either complainant. It stated that the numbers were obtained from its system of all active members but that they should not have been included in the marketing campaign. It also informed us that it was not aware that the opt-out option should have been included in the original text message as it always sent a follow up opt out text message. Having probed this matter further with the service provider who sent the text messages on the Leisure Club's behalf, there was no evidence to suggest that a follow up opt out message was sent to the complainants. The complainants also informed us that they did not receive such follow up opt out messages. It was clear to us that Citywest Health and Leisure Club had not heeded our previous warning letter of August 2010. The Commissioner decided, therefore, to take prosecutions against Citywest Resort Limited in relation to these offences.

On 19 November 2012, Citywest Resort Limited faced forty six charges at the Dublin District Court. It pleaded guilty to the sending of unsolicited marketing text messages to the two complainants without consent. Citywest Resort Limited was convicted on two counts and a fine of €1,000 was imposed. The prosecution costs were recovered from the defendant.

Therapie Laser Clinics Ltd

In 2010 we received a number of complaints about Therapie Laser Clinics Ltd in relation to the sending of unsolicited marketing text messages without consent and without an opt out facility. In some cases, the marketing messages promoted a sister company, Optilase. Following our investigation, Therapie assured us at the time that it would remove each complainant's mobile phone number from its database. We issued a formal warning to Therapie in early 2011 to the effect that any further offences committed would be prosecuted.

In 2012 we received two further complaints regarding unsolicited marketing text messages sent by Therapie. One of the complainants was among those who complained in 2010 in relation to the issues described above. The second complainant stated that he had never given his mobile phone number to Therapie previously.

In response to our investigation, Therapie informed us in March 2012 that it was unable to confirm whether marketing text messages were sent to one complainant's phone as it could not see the number on its system. We requested information from Therapie's text service provider in relation to the text messages sent to the complainant. It informed us that Therapie had sent it an email requesting that the complainant's number be removed form the database. This email was sent on the very same date on which Therapie informed us that it could find no record of the complainant's number.

The Commissioner decided to prosecute Therapie on eight charges. In the Dublin District Court, the defendant entered a guilty plea on four charges. The Court convicted the defendant on two charges and it took two charges into account. It imposed a total fine of €4,000. The prosecution costs were recovered from the defendant.

Mobile Phone Companies

On 3 December 2012, we prosecuted the following companies at the Dublin District Court.

*Meteor Mobile Communications Limited (T/A Meteor)*

On the basis of one complaint from a member of the public we summoned Meteor Mobile Communications Limited on seven charges. The company pleaded guilty to one charge of sending an unsolicited marketing text message without consent. Meteor stated that due to human error the normal protocols were lifted in relation to a particular marketing campaign. This resulted in the complainant receiving an unsolicited marketing text message despite being previously opted out.

Of significant concern was the fact that Meteor admitted that unsolicited marketing text messages were sent to between 11,000 and 18,500 individuals due to this human error.

The Court ordered Meteor to make a charitable donation of €5,000 to the Children's Hospital in Temple Street and the Probation of Offenders Act was applied. The prosecution costs were recovered from Meteor.

*Hutchison 3G Ireland Limited*

Hutchison 3G Ireland Limited (Three) entered guilty pleas in respect of three out of seven charges for offences concerning an unsolicited marketing text message, an unsolicited marketing email and an unsolicited marketing phone call to different individuals.

In the first case, the complainant received an unsolicited text message to his mobile phone number. This person had previously opted out of receiving marketing communications from Three.

In the second case, the complainant was a former customer of Three who had requested that no direct marketing contact be made to her in any form. Due to what was described as a coding error an unsolicited marketing email was sent to the complainant without consent.

In the third case, the complainant had opted out of receiving marketing phone calls. He received a marketing phone call from a representative on behalf of Three.

The Court ordered Hutchison 3G Ireland Limited to donate €2,500 to the Children's Hospital in Crumlin and the Probation of Offenders Act was applied. The Office's prosecution costs were recovered from the defendant.

*The Carphone Warehouse Limited*

The Carphone Warehouse Limited entered guilty pleas in respect of two out of ten charges relating to the sending of unsolicited marketing emails to two individuals.

In both cases the complainants received unsolicited direct marketing emails without having been opted in to receive same.

The Court convicted The Carphone Warehouse Limited on both counts and it imposed a fine of €1,250 in each case. The prosecution costs were recovered from the defendant.

***Case Study 13 Stolen Laptops - Phone Companies Prosecuted For Loss of Personal Data***

In the first prosecution case of its kind in Ireland, two telecommunications companies, Eircom and Meteor, appeared in the Dublin District Court in September 2012 to face charges relating to the loss of customer personal data which was stored on two unencrypted laptops, which had been stolen several months previously.

**Background**

A data breach report was received by this Office on 2 February 2012 from Eircom and Meteor. Regulation 4(6) of SI 336 of 2011 obliges telecommunications companies to notify the Data Protection Commissioner of personal data breaches without undue delay. This Regulation also obliges telecommunications companies to notify affected individuals of a data breach where the said breach is likely to adversely affect their personal data or privacy. The breach report informed us that two unencrypted laptops had been stolen from Eircom's offices at Parkwest in Dublin between 28 December, 2011 and 2 January, 2012. The report confirmed that the stolen laptops contained information relating to customers, including personal data. It indicated that the number of affected customers were 454 in the case of Meteor and 6,597 in the case of eMobile. The theft of the laptops was discovered on 3 January, 2012 and the matter was reported to the Gardai (national police force) on 4 January, 2012. The breach report was made thirty days after the laptops were reported as stolen. An updated breach report was submitted on 15 March, 2012. This followed intensive contact between ourselves and eircom/Meteor including two meetings on site. The report indicated that, following a second phase of internal investigation, it was found that the number of affected customers was greater than previously reported. The revised figures were 3,944 Meteor customers and 6,295 eMobile customers.

**Eircom (trading as eMobile)**

6,295 eMobile customers were affected by the data breach. In relation to 142 of these cases, the personal data in question was in the form of customer application forms including proof of identity (e.g. copy of passport, driving licence, national identification, bank account/credit card details, financial statements and utility bills).

The other 6,153 cases contained details such as name, address, telephone and account number. The process of Eircom notifying its affected customers by letter began on 10 February 2012 (38 days after the laptops were reported stolen). A large number of affected customers were notified for the first time on 20 March, 2012 (77 days after the laptops were reported stolen). Letters included an apology to customers for the loss of their personal data. At our request, Eircom notified the banks of the breach via the Irish Banking Federation on 9 February, 2012.

**Meteor**

3,944 Meteor customers were affected by the data breach. In relation to approx 1,244 of these cases the personal data in question was in the form of proof of identity documents (e.g. copy of passport, driving licence, national identification, Bank Account/Credit Card details, financial statements and utility bills). The other 2,700 cases approx contained details such as name, address and telephone and account number. The process of Meteor notifying its affected customers by letter began on 10 February 2012 (38 days after the laptops were reported stolen). An update of the 10 February, 2012 letter was issued on 20 March, 2012. A large number of affected customers were notified for the first time on 16 March, 2012 (73 days after the laptops were reported stolen). Letters included an apology to customers for the loss of their personal data. At our request, Meteor notified the banks of the breach via the Irish Banking Federation on 9 February, 2012.

**Data Security**

In relation to the electronic communications services sector, Regulation 4(1) of SI 336 of 2011 places an obligation on providers to take appropriate technical and organisational measures to safeguard the security of their services. Regulation 4(2) details some requirements specific to the electronic communications services sector. It provides that the measures to ensure the level of security shall at least ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, protect personal data stored or transmitted from access or disclosure and ensure the implementation of a security policy with respect to the processing of personal data. We published a comprehensive guidance note on data security on our website in August, 2010. This included guidance to the effect that encryption is considered an essential security measure where personal data is stored on a portable

device or transmitted over a public network. Encryption is the method of converting data from a readable format to an unreadable or unintelligible format so that unauthorised persons are unable to access the data. On a portable device such as a laptop, encrypting data is a method of securing the data to protect it from access by unauthorised persons in the event that the device on which the data is stored comes into the possession of unauthorised persons.

Following this breach, the Eircom Group identified approximately 160 laptops which were not encrypted. All unencrypted laptops were encrypted by 24 February, 2012.

**Breach Notification**

This Office considers that data breaches of this nature should normally be reported to us within two working days of the data controller becoming aware of the incident. This has been our stated position since a data security breach Code of Practice was published in July 2010. Once we are notified of a breach we can quickly advise the data controller of what steps to take, what areas to focus on, how best to notify affected parties quickly, whether other bodies such as banks need to be informed of the breach, etc. Notification of a data breach to affected individuals quickly is also critical and essential as it allows them to take remedial action to protect themselves and their identities – particularly in cases where financial and identification documentation is stolen.

**Court Hearing**

At the Dublin District Court on 10 September, 2012 guilty pleas were entered on behalf of each defendant, Eircom and Meteor, in relation to three charges each in respect of offences under Regulation 4(1), Regulation 4(6)(a) and Regulation 4(6)(b) of SI 336 of 2011. These charges related to the failure to protect the personal data on the laptops by means of encryption, the failure to notify the Data Protection Commissioner of the data breach without undue delay and the failure to notify the affected customers of the data breach without undue delay. After hearing the prosecution evidence, the Court was satisfied that the prosecution case was proven. The Court applied Section 1(1) of the Probation of Offenders Act, conditional upon a charitable donation of €15,000 being made by each Defendant to charities nominated by the Court - the Laura Lynn Foundation in the case of Eircom and Pieta House in

the case of Meteor. This Office also recovered from the defendants the legal costs arising from the prosecution.

***Case Study 14: Client list taken by ex-employee to new Employer***

This personal data security breach involved two car showrooms based in the same locality. Garage A notified this Office of a data security breach under the Code of Practice. Garage A was alerted to the fact that one of their customers had received a marketing letter from a former employee who was now working for Garage B. The letter stated that the employee had moved to a different employer and was promoting Garage B.

Our investigation into this matter focussed on the issues of Garage A failing to keep secure the personal data that it held and that of Garage B processing personal data for which it had no consent to process.

When we contacted Garage B in relation to their processing of data relating to customers of Garage A, Garage B stated that the data had been contained within the diary of the new employee. The employee had used this data to write to individuals with whom he had dealt with as an employee of Garage A. It was clear that Garage B had no consent from the individuals to process their data or to send marketing communications. Garage B also informed my Office that the data in question had now been destroyed.

Our Office also examined the data protection provisions in the employee contract of Garage A. The contract referred to the use of business data. We recommended to Garage A that the contract be amended to include specific reference to the use of personal data to prevent any ambiguity.

In certain situations that have come to our attention, there appears to be a misconception by some employees that the customers are their customers rather than that of the data controller, i.e. the employer. Data controllers must be aware that where they process data which has been brought in to the organisation by a new employee from their previous employment, without the consent of the individuals, they are in breach of the Data Protection Acts. This could be further exacerbated if they engage in electronic marketing to those individuals.

***Case Study 15: <u>Allied Irish Banks – postal breaches</u>***

During the Office's investigation into the cause of postal breaches, it was identified that a significant proportion of Allied Irish Banks' (AIB) breach notifications were the result of changes of address not being fully processed. We contacted AIB to raise the issue and to seek a solution. The response from AIB showed the seriousness with which they treated the matter, including bringing this matter to the attention of its Board Risk Committee.

AIB stated that it deals with, on average, 240,000 address amendments each year. However, almost one third of the notifications made by AIB to this Office were the result of errors made in the processing of such requests.

AIB, on foot of contact from this Office, carried out a comprehensive analysis of each incident to establish the cause of the error. AIB has now notified us of the procedures it is putting in place to address this issue.

AIB is to introduce a number of measures including the introduction of a "Self-Service Change of Address" facility on its internet banking portal to allow account holders to amend or change their address on accounts held solely in their name. A central unit to process address amendment requests is also to be established. It is proposed that change of address notifications will first be directed towards the self-service facility, but where this is not an option or appropriate, the notification will be forwarded to the central unit for processing.

AIB has also informed us of a number of additional steps that it will be taking immediately, including a number of training and briefing sessions to all its staff and the introduction of additional internal controls.

This Office welcomes the steps being taken by AIB to address this issue. We will monitor the effects of these new procedures and it is expected that they will lead to a serious reduction in the number of such data breach notifications that require to be made to the Office.

***Case Study 16: <u>Major Retailer – Credit card slips discarded</u>***

Early in the year, the Office received calls from two individuals reporting that there were credit card receipts littering a housing estate. The individuals had collected some of the receipts and were able to identify the retailer and the branch involved. We immediately contacted the retailer to advise them of the matter and to ensure that the retailer immediately sent staff to the area to recover the receipts.

The Retailer later notified this Office that the issue occurred when an envelope containing customer signed credit card receipts was put out for recycling rather than being securely destroyed. The envelope was then left out overnight in the store's recycling bin. It is assumed that a passer-by searched through the bin, found and took the envelope. The individual then discarded the contents of the envelope a distance away from the store.

The Retailer, in an effort to recover the credit card slips, had staff search the locality in which the slips were seen and call to houses to recover any slips that may have been collected by individuals. The Retailer retrieved 500 credit card slips and was able to determine the period in which the relevant purchases had been made. We queried the total number of slips that were collected by the Retailer in this period.
It was determined that there was a balance of 200 receipt slips unaccounted for. Of the 500 recovered by the Retailer, many had been damaged by the inclement weather at the time and the details of the card holder could not be identified.

In dealing with such data security breaches, this Office employs a three-pronged approach. Firstly, we recommend that the affected individuals be notified of the matter. Secondly, the data controller should take steps to recover / secure the data. Finally, the data controller must put in place procedures to prevent a repeat of the issue.

In this case, the Retailer would not have the contact details of the affected individuals, nor was it in a position to identify all the affected individuals. The Retailer therefore contacted its service providers who process the credit and debit card payments. The

card processing companies were able to identify the 700 customers involved. It was not appropriate for the card processing companies to supply the contact details to the Retailer and the card processing companies stated that in circumstances such as this it was their practice to monitor accounts for potential fraudulent activity, but not notify the cardholders directly. It was therefore agreed to proceed on this basis, the Retailer bearing all charges associated with this monitoring.

The Retailer, in attempting to secure the data, assigned considerable resources to searching the area in which the receipts slips were discarded and canvassing local houses. As noted above, this resulted in 500 of the 700 slips being recovered.

The Retailer notified my Office of the new procedures it was employing to prevent a repeat of this incident. A review of all confidential information held in stores was carried out and a special collection was arranged from all stores for the disposal of such information. A notification was issued to all staff reminding them of the need to securely store or destroy such confidential material. The Retailer's Data Protection Policy and disposal policy were also updated.

We had also identified that the receipts being printed by the Retailer contained the full card number and start and expiry date of the card. We brought this issue to the attention of the Retailer, raising concerns with such a practice. The Retailer confirmed to this Office that it was changing its practice and future receipts would be printed with only part of the card number visible.

***Case Study 17: <u>O2 – Missing media tape</u>***

Under the requirements of S.I. 336 of 2011, O2 notified the Office of a data security breach involving a missing backup media tape in July.

O2 stated that the tape had been identified as missing by its service provider, IBM, in February. IBM had conducted searches for the missing backup media tape but was unable to locate the tape and notified O2 of the matter in May.

In their notification to this Office, O2 stated that the data held on the media tape could only be accessed using the same technical equipment utilised to create the tape, which would cost in excess of €600,000.

We investigated this claim and found evidence contrary to the claim of O2. We then informed O2 of our findings, requested details of the type of data held on the backup media tape, and informed O2 of the need to notify affected individuals.

O2 reverted stating that the backup media tape was created in August, 2011 and it no longer held records as to what was held on the media tape. It was therefore not in a position to identify the type of data held on the tape and the affected individuals.

We also sought an explanation as to the delay in notifying our Office of the data security breach. Under the obligations imposed by S.I. 336 of 2011, Telecommunications companies & ISP's are required to notify both this Office and affected individuals without undue delay.

O2 explained that they had not been notified by their service provider of the data security breach until 3 months after the issue was identified. The service provider during this time was carrying out searches for the missing media tape and analysing the potential issues. We informed O2 that this delay was unacceptable.

O2, as part of their report to the Office, provided two separate external forensic analysis reports on the backup media. Both of these reports examined the possibility of a third party gaining access to the data held on the missing media tape. Both reports stated that the data could not be accessed by an individual without access to proper equipment and technical expertise. O2 therefore argued that the data on the media was unintelligible, given the requirements to access the data. However, this Office pointed out that both external reports supplied by O2 did note that the data could be accessed by a third party with sufficient resources. As the data was potentially accessible, Regulation 4(6)(b) of S.I. 336 of 2011 applied, requiring notification of affected individuals. The appropriate standard to be applied is not whether a member of the public could access the data, but whether the data could be accessed at all.

Whilst O2 disagreed with the views and interpretation of this Office, they agreed, as a matter of goodwill, but without any acknowledgement of liability or failure under the Data Protection Acts or S.I.336, to make a charitable donation and notify customers of the matter.

As O2 were unable to identify specifically affected individuals, it was agreed that they would make a public announcement of the matter, via their website and press release. This announcement was made in early December. O2, as a gesture of goodwill, also made a charitable donation of €50,000 to Headstrong, a non-profit organisation supporting young people's mental health.

To ensure that this type of data security breach did not occur again, O2 had undertaken a number of steps, including improved security and controls regarding the storage of media tapes. The Office also made a number of recommendations to O2, including the encryption of its backup media and that the contract between O2 and its third party service providers be amended to include a requirement for immediate notification of any potential data security breaches.

***Case Study 18: <u>Health Service Executive</u>***

In February, the Health Service Executive (HSE) reported to this Office a data security breach involving the disclosure of patient data to a third party. Documents which were faxed to the Assisted Admissions Services from a number of Mental Health Services were faxed to a private company in error. The company alerted the HSE to the issue, stating that it had received approximately 100 such faxes over a 3 year period. It had destroyed each fax as received but had not alerted the HSE to the issue until that point. The company stated that it had 20 such faxes in its possession which it had recently received and the HSE immediately organised to collect these documents from the company.

The HSE employs a third party company to provide assisted admissions services in certain geographic areas. The issue arose when staff incorrectly entered the wrong fax number when sending such faxes, dialling the Dublin area code number rather than the correct county code number.

This Office notified the HSE of its alarm at the fact that this type of breach was occurring, especially in light of previous communications with the HSE regarding the sending of sensitive data by fax. This Office had recommended a number of measures, including that the sender should first contact the recipient to expect the fax and that the sender should ensure that the fax number is dialled correctly.

The HSE responded to this Office notifying that the investigation into the matter had been escalated to its National Incident Management Team. The HSE stated that it was pre-programming the number of the Assisted Admissions Unit into all relevant fax machines. Old fax machines were replaced and additional machines provided in areas that did not have specific access to a fax machine.

The issue had appeared to have been addressed when the HSE notified this Office in August of another such incident. The HSE notified this Office that the pre-

programmed number on the relevant fax machine had disappeared from the pre-programmed number list. The HSE further informed us that it was now introducing a specific 1800 fax number for the Assisted Admissions Unit. It has also changed the number dialled to access an outside number from zero to nine, to reduce the risk of an individual mis-dialling a number. This Office also advised that a sticker with the fax number of the Assisted Admissions Unit be placed on each fax machine. The HSE policy document in relation to the use of fax machines has also been displayed beside each fax machine within the HSE.

We were disappointed that this issue arose in the first instance, especially in light of previous communications with the HSE, and to then have it reoccur during the year, after the HSE had introduced preventative measures. It is apparent that staff were not adhering to the procedures which had been introduced. This issue highlights that, while data controllers can put in place systems to address potential data protection matters, all staff must be properly informed of the procedures being introduced and adhere to them.

## Appendices

Appendix 1 – Presentations

Appendix 2 – Registration statistics

Appendix 3 – Account of income and expenditure

Appendix 4 – INFOSYS Investigation

## *Appendix 1- Presentation and Talks*

During 2012 we gave 76 presentations to the following Organisations

American Bar Association (webinar)
Association of Compliance Officers of Ireland x 2
Chartered Accountants Ireland
Citizens Information Board
Cloud Security Alliance
Credit Union Managers Association x 2
Cybercrime Summit
Data Protection Seminar
Department of Justice & Equality x 2
Digital Childhoods Seminar
Digital Hub Development Agency
Digital Rights Forum
Digital Youth Symposium
Dublin Solicitors Bar Association x 2
eGovernment Seminar
Environmental Health Officers Association
European Commission x2
European Commission (TAIEX) x2
European Commissioners Conference
European Data Protection Lawyers Forum
European Parliament
Fidelity Investments
Forum Europe
Heanet
HSE – Research Ethics Committees Member Training
Hungarian DPA Hosting Case Handling Workshop
Independent Hospitals Association of Ireland
Industrial Development Authority
INSAFE Network
Institute of Public Administration x 2
Institution of Occupational Safety and Health
Intelligent Transport Systems Ireland
International Association of Privacy Professionals x3
International Bar Association
International Chamber of Commerce UK ePrivacy Event
Internet Service Providers Association
Intertrade Ireland ICO
Irish Association of Social Workers
Irish Computer Society
Irish Institute of Credit Management
Irish League of Credit Unions

Irish Payroll Association
ISACA
ITS Ireland
Law Society Conference "21st Century Technology
Legal Island
Local Government FOI Network
Mater Dei Institute
PDP Practical Compliance Conference
Professional Insurance Brokers Association (PIBA)
Public Affairs Ireland x4
Public Service Internal Audit Conference
RCPI
RCSI Clinical Research Nurse Programme
Rotary Club
Royal Irish Academy
Royal Irish Academy Realising the Opportunities of Digital
TEEU
Trinity College School of Computer Science and Statistics
Twin Cities Privacy Forum (USA)
UCD
Union of Students in Ireland
Walkers Solicitors
Youth Work Ireland

*Appendix 2 - REGISTRATIONS 2012*

**The total number of register entries in 2012 was 5,338. This figure can be broken down into the following categories:**

(a) Financial and Credit Institutions

614

(b) Insurance Organisations

400

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

122

(d) Telecommunications / Internet Providers

50

(e) Health Sector

1349

(f) Pharmacists

1072

(g) Miscellaneous

373

(h) Data Processors

1358

**Total number of registration entries**

| **2010** | **2011** | **2012** |
|---|---|---|
| **4954** | **4940** | **5338** |

**In 2012 the number of organisations registered increased by 398 approximately 8%. This increase arose due to a targeted awareness campaign by us on the Insurance sector and also our pursuit of the cases which had gone off the Public Register during 2012.**

***Appendix 3 - Abstract* of Receipts and Payments in the year ended 31 December 2012***

**Account of Receipts and Payments in the year ended 31 December 2012**

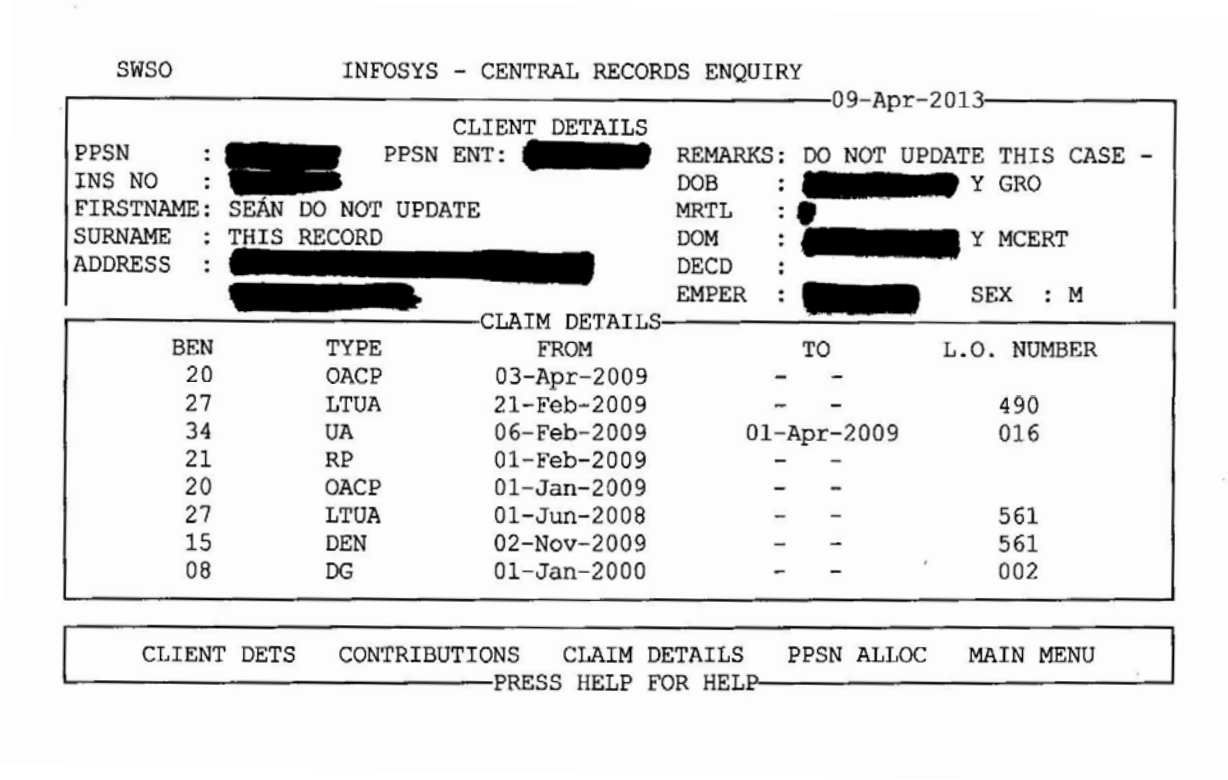
| **Receipts** | **2012 €** | **2011 €** |
|---|---|---|
| Moneys provided by the Oireachtas | 1,552,468 | 1,449,962 |
| Fees | 643,896 | 616,463 |
| Other Receipts | 3,825 | 887 |
| | **2,200,189** | **2,067,312** |
| Payments | | |
| Staff Costs | 1,265,509 | 1,224,116 |
| Establishment Costs | 68,232 | 70,972 |
| Legal and Professional Fees | 210,233 | 144,349 |
| Miscellaneous Expenses | 8,494 | 10,525 |
| | 1,552,468 | 1,449,962 |
| Payment of receipts for the year to the Vote for the Office of the Minister for Justice and Equality | 635,428 | 588,477 |
| Receipts payable to the Vote for the Office of the Minister for Justice and Equality at year end | 12,293 | 28873 |
| | **2,200,189** | **2.067,312** |

**The figures for 2012 outlined above are still subject to audit by the Comptroller and Auditor General. The final audited accounts will be presented to the Minister for Justice & Equality for presentation to the Oireachtas*

*Appendix 4 – INFOSYS Investigation*

# INFOSYS

## An investigation by the Office of the Data Protection Commissioner into the use of INFOSYS outside of the Department of Social Protection



SWSO INFOSYS - CENTRAL RECORDS ENQUIRY

09-Apr-2013

CLIENT DETAILS

PPSN : [redacted] PPSN ENT: [redacted] REMARKS: DO NOT UPDATE THIS CASE -
INS NO : [redacted] DOB : [redacted] Y GRO
FIRSTNAME: SEÁN DO NOT UPDATE MRTL : [redacted]
SURNAME : THIS RECORD DOM : [redacted] Y MCERT
ADDRESS : [redacted] DECD :
[redacted] EMPER : [redacted] SEX : M

CLAIM DETAILS

| BEN | TYPE | FROM | TO | L.O. NUMBER |
|---|---|---|---|---|
| 20 | OACP | 03-Apr-2009 | - - | |
| 27 | LTUA | 21-Feb-2009 | - - | 490 |
| 34 | UA | 06-Feb-2009 | 01-Apr-2009 | 016 |
| 21 | RP | 01-Feb-2009 | - - | |
| 20 | OACP | 01-Jan-2009 | - - | |
| 27 | LTUA | 01-Jun-2008 | - - | 561 |
| 15 | DEN | 02-Nov-2009 | - - | 561 |
| 08 | DG | 01-Jan-2000 | - - | 002 |

CLIENT DETS CONTRIBUTIONS CLAIM DETAILS PPSN ALLOC MAIN MENU

PRESS HELP FOR HELP

**May 2013**
**Office of the Data Protection Commissioner**

# Contents

## Executive Summary

In 2008, the Office of the Data Protection Commissioner conducted an audit of the Department of Social Protection. Key areas within the Department were selected for close examination, some targeted and some random. The audit report is available to view or download from the Department of Social Protection's website[7].

Since the audit took place, the Office has continued to deal with the Department of Social Protection frequently on a number of fronts such as the rollout and implementation of the public services card, data protection policy and procedures, internal audit investigations and liaising with this Office in relation to any reported data breaches (including any cases of inappropriate employee access to personal data).

During the course of the 2008 audit, the Audit Team examined INFOSYS - a 'read-only' portal allowing access to data held on a range of Department of Social Protection databases providing information on individuals, their partners and their dependants in terms of any benefits or allowances they may be in receipt of from the Department. The deployment of generic user accounts to access INFOSYS both internally within the Department and externally emerged as an area of particular concern in the 2008 audit report. Specifically, the report noted the number of external agencies with 'read-only' access to INFOSYS.

As well as the findings and recommendations featured in the 2008 audit report, the Office decided to examine external access to INFOSYS further in the light of a major investigation into abuse within the Department of Social Protection in terms of one employee's access patterns. A criminal investigation is currently underway by An Garda Síochána with regard to this Department of Social Protection employee who allegedly accessed social welfare records and passed the information onto private investigators. This particular investigation also led to the successful prosecution by this Office of a number of insurance companies[8] who processed the illegally acquired data. The investigation ultimately led this Office to query whether similar abuse might occur in locations where external access to social welfare data via INFOSYS had been granted to specified bodies.

The Office therefore decided to commence an investigation under Section 10 of the Data Protection Acts into the compliance by each of the external bodies granted access to INFOSYS with their responsibilities under the Acts to appropriately manage such access. The investigation commenced in the second quarter of 2011 and continued on throughout 2011 and 2012. Full co-operation was by and large received from all organisations contacted in connection with our investigation.

A worrying degree of inappropriate access to INFOSYS by state employees was detected as a result of the investigation conducted by the Office. Some of this misuse was uncovered through internal investigations initiated by the agencies themselves. In other cases, inappropriate access was identified during the course of our examination of the access logs and subsequent engagements with these entities

[7] http://www.welfare.ie/EN/Topics/Documents/ODPCReport.pdf

[8] FBD Insurance Plc, Zurich Insurance Plc, and Travelers Insurance Co. Ltd — each pleaded guilty to 10 sample charges under the Data Protection Act after they illegally acquired access to social welfare records. A significant number of customers of these companies had information such as employment histories, claims data and PPS numbers illegally obtained.

including physical on-site inspections. In particular, we uncovered cases of inappropriate access within the HSE that indicated an unacceptable lack of awareness within the HSE as to what actually constituted inappropriate access.

While the Office is satisfied that no entity investigated sought to deliberately breach the provisions of the Data Protection Acts regarding use of INFOSYS, it is nevertheless the case that the actions of a number of authorised users across the spectrum of specified bodies granted access to INFOSYS breached the Acts. A key purpose of this report therefore is to clarify exactly what the requirements of the Data Protection Acts are in this area. It is expected that all users of INFOSYS will move to immediately amend their procedures accordingly. Implementation of the recommendations contained in this report will be subject to close scrutiny.

Another aspect of the INFOSYS Investigation was the exchange of data between agencies in instances where fraud or illegal activity became evident as a result of information obtained on INFOSYS being combined with information already in the agency's possession. Having reviewed the pertinent legislation, we are of the view that sections 261(2), 261(3) and 265 of the Social Welfare (Consolidation) Act 2005 provide a legal basis for the request and exchange of data between the Department of Social Protection and other specified public bodies. However, the extent and proportionality of data sharing in the public sector have remained a constant source of concern to this Office and we consider there is a need for the Department of Social Protection to review the permitted purposes for which INFOSYS information may be accessed and used, especially by local authorities.

Finally, it is important to make clear from the outset of the INFOSYS investigation report that the Department of Social Protection was not the focus of the INFOSYS investigation but clearly deficiencies identified in how the external bodies are managing access to the Department's systems now requires the Department of Social Protection to initiate corrective action.

## Key Recommendations

### Fair Obtaining & Processing

- An agency's facility to directly access and check Department of Social Protection data must be directly referenced on all relevant scheme documentation used by entities granted external access to INFOSYS. It should be abundantly clear to members of the public that their compliance with statutory requirements, applications and eligibility details for a range of schemes may be checked on social welfare databases using INFOSYS. The precise legal basis allowing these checks to take place should be cited alongside such notices.

### Purpose Limitation

The practice whereby agencies' users are conducting checks on INFOSYS for purposes outside of those agreed with the Department of Social Protection and captured in memoranda of agreements between the Department and each agency must cease immediately. The Department of Social Protection should critically review the purposes for which access to INFOSYS is permitted with a view to ensuring that access for such purposes is proportionate.

## Further Processing/Disclosure

- Every organisation authorised to access INFOSYS should maintain a register of all requests for disclosure and information received and issued. All information received from or passed onto external bodies such as Revenue, Department of Social Protection and An Garda Síochána should be noted by each authorised agency.

- All requests should be made in writing (or followed up in writing) and these requests recorded with a copy of correspondence issued and received.

## Security

- The practice whereby authorised users are conducting checks on INFOSYS for purposes outside of those captured in memoranda of agreements with the Department of Social Protection and signed data protection declarations by the users themselves must be subject to a comprehensive set of preventative measures and a set of procedures that can be invoked in the event of such abuse being detected. Any inappropriate employee access identified should incur severe disciplinary penalties, including monetary penalties where warranted.

- All inappropriate access identified by management should be reported to the Office of the Data Protection Commissioner as a data breach as per guidance contained in the **Personal Data Security Breach Code of Practice**[9] published by this Office in July 2011 to help organisations to react appropriately when they become aware of breaches of security involving customer or employee personal information. It is imperative for organisations to understand that data breaches include all instances of inappropriate employee access.

- The Department of Social Protection needs to make available as a matter of priority a reporting tool to all agencies with access to INFOSYS to allow these agencies to check on the appropriateness of such access to individual user accounts.

- Once the tool is provided to each agency they must embark upon a programme of pro-active monitoring of all access within their organisation to INFOSYS. In the interim, all agencies should conduct spot-checks of employee access facilitated by the secure provision of user logs by the Department of Social Protection. These checks should be documented so that evidence of such checks can be noted and reviewed by this Office.

- All users of INFOSYS should be made aware of these random spot checks and the consequences for them if inappropriate employee access to data held on INFOSYS is detected.

- In conjunction with the existing built-in-mechanism whereby an individual staff member's access to INFOSYS is automatically suspended after a certain period of inactivity, the designated point of contact for each agency authorised to use INFOSYS should also run a quarterly report, detailing all users who have not accessed INFOSYS. Such reports enable each agency to identify redundant users and ensure their accounts are permanently shut down.

[9] http://www.dataprotection.ie/docs/07/07/10_-_Data_Security_Breach_Code_of_Practice/1082.htm

- Consideration must be given to the different requirements of each type of user approved to access INFOSYS and their access privileges to personal data should fully reflect these requirements. The nature of access allowed to an individual user should be set and reviewed on a regular basis. Individual staff members should only have access to data which they require in order to perform their duties.

## 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 with particular emphasis placed on the safeguarding of 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 use and purposes of INFOSYS within their own organisations. These procedures need to make clear when it is legitimate to access INFOSYS and when it is not. The procedures also need to clearly stipulate the monitoring arrangements 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 regarding access and the use of INFOSYS are in line with the requirements of the Data Protection Acts 1988 & 2003.

INFOSYS is a 'read-only' portal allowing access to data held on a range of Department of Social Protection databases. Access to INFOSYS is granted by the Department of Social Protection to certain authorised state bodies to allow them to check social welfare data against data supplied in applications an individual might make to schemes such as the medical card scheme, the fair deal Nursing Homes Support Scheme, or the local authorities Rental Accommodation Scheme (RAS). In other contexts, access to INFOSYS allows labour inspectors to check the employment details of employees or employers and statisticians in the Central Statistics Office to check the veracity of data supplied as part of its annual income and living conditions survey.

The report has been structured in such a manner as to map the investigation and findings chronologically, beginning with an overview of the actual system itself (INFOSYS). The report than provides an overview of the various sectors investigated i.e., HSE, local authorities, the Central Statistics Office and the National Employment Rights Agency (NERA).

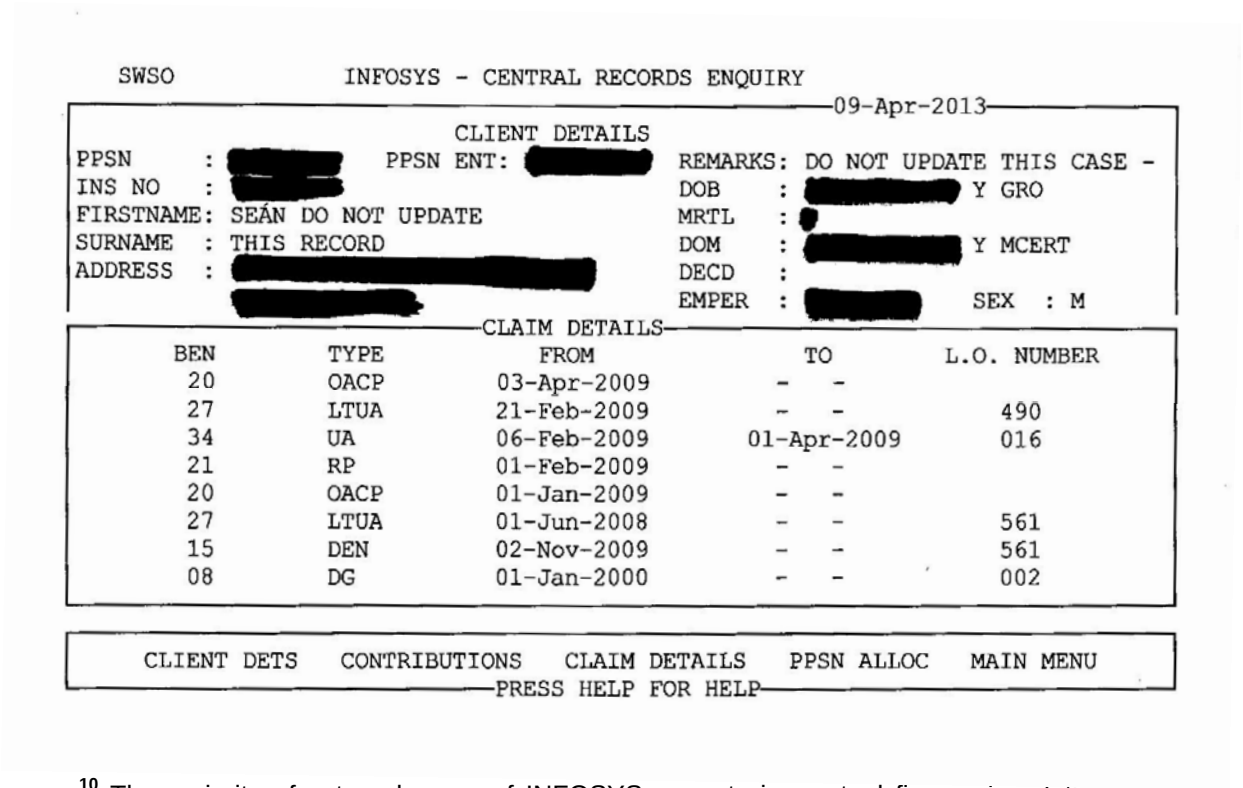
# 1. INTRODUCTION

## 1.1 What is INFOSYS?

There are over 50 live systems within the Department of Social Protection containing the personal data of customers and staff members of the Department. The principal database feeding into many of these systems is the Central Records System (CRS) which holds in excess of 7.7 million client records. It is the Department's central database for holding customer records. Query access to this system and all other systems is generally managed through what is known as the INFOSYS system.

INFOSYS is a query system used to view the details of a client's record across most of the Department of Social Protection's (DSP) transaction systems. The application consists of a snapshot of payment and record information held by the DSP and is a read-only system which cannot be altered by those accessing it. INFOSYS is the standard access tool to social welfare data used by staff working in the Department of Social Protection. User access to INFOSYS is assigned similar to the Central Records System, with querying limited to the level of access assigned to the user by their business manager.

If a search is run on an individual on INFOSYS, summary details of the type of social welfare benefits and the overall means of social welfare recipients and their dependants will appear in the search results (see table below). This data may be of relevance or interest in the context of an application to a scheme being handled by one of the authorised entities. Social Welfare databases are also populated with data feeds from Revenue in relation to employment data and earnings[10].



SWSO INFOSYS - CENTRAL RECORDS ENQUIRY

09-Apr-2013

CLIENT DETAILS

PPSN : [redacted] PPSN ENT: [redacted] REMARKS: DO NOT UPDATE THIS CASE -
INS NO : [redacted] DOB : [redacted] Y GRO
FIRSTNAME: SEÁN DO NOT UPDATE MRTL : [redacted]
SURNAME : THIS RECORD DOM : [redacted] Y MCERT
ADDRESS : [redacted] DECD :
[redacted] EMPER : [redacted] SEX : M

CLAIM DETAILS

| BEN | TYPE | FROM | TO | L.O. NUMBER |
|---|---|---|---|---|
| 20 | OACP | 03-Apr-2009 | - - | |
| 27 | LTUA | 21-Feb-2009 | - - | 490 |
| 34 | UA | 06-Feb-2009 | 01-Apr-2009 | 016 |
| 21 | RP | 01-Feb-2009 | - - | |
| 20 | OACP | 01-Jan-2009 | - - | |
| 27 | LTUA | 01-Jun-2008 | - - | 561 |
| 15 | DEN | 02-Nov-2009 | - - | 561 |
| 08 | DG | 01-Jan-2000 | - - | 002 |

CLIENT DETS CONTRIBUTIONS CLAIM DETAILS PPSN ALLOC MAIN MENU

PRESS HELP FOR HELP

[10] The majority of external users of INFOSYS cannot view actual figures in relation to an individual's private income or total earnings. However, data regarding an individual's income can be sought and shared on a case-by case basis between public sector bodies under a range of legislative provisions.

During the course of the investigation it was noted that it is possible to search INFOSYS using a range of criteria such as PPSN, surname, address and even 'Relationship Detail' which allows for information on individuals to be accessed relatively easily.

Search results on INFOSYS may lead to an application being unsuccessful if it is concluded that information materially relevant had not been disclosed initially at the application stage. Search results on INFOSYS can also assist a range of agencies such as local housing authorities, the HSE and labour inspectors in NERA to detect fraud or failure to comply with statutory requirements.

## 1.2 2008 Audit of the Department of Social Protection

We conducted a general compliance audit[11] of the Department of Social Protection in 2008 leading to the instigation of a more targeted series of investigations in 2011 and 2012, based on concerns in relation to the monitoring and control of external access to INFOSYS and the compliance of such activity with the Data Protection Acts.

Issues of specific note in the 2008 audit report of the Department of Social Protection in relation to INFOSYS centred on the allocation of generic user accounts both internally within the Department and externally. The large number of external agencies with access to INFOSYS was also noted.

A key recommendation of the 2008 audit report was to

> "Immediately disable generic accounts, e.g., as found in relation to INFOSYS and put a policy in place to prohibit the use of such accounts to access DSFA data. Create unique accounts only that will provide for a meaningful audit trail". (p.28)

By the end of the audit process, this Office was assured in the final version of the audit report that

> "all generic access to the INFOSYS and CRS systems have now been removed within the Department" (p. 8).

With regard to external access using generic accounts, the final audit report stated that

> "arrangements are underway to disable all external generic accounts containing customer data" (p.28).

It was also stated in the 2008 audit report that

> "The Department has also requested the HSE to conduct an audit of INFOSYS and ISTS accounts to ensure that only staff who require access to these systems are provided with it." (p.17)

[11] http://www.welfare.ie/EN/Topics/Documents/ODPCReport.pdf

*[In response to this, the Department of Social Protection clarified that in 2012, Client Identity Services in DFSA reviewed all ISTS[12] account holders in the HSE. All ISTS accounts held by HSE staff that did not transfer into the DSP were deleted (approx. 130 accounts)]*

At the time of the audit in 2008, we noted that all activity including read-only access to records through INFOSYS was logged and a complete audit trail of all 'look-ups' was retrievable. This in-built audit trail functionality was to prove crucial throughout the INFOSYS investigation. Audit trail functionality incorporating all 'look-ups' on a system where unique logins are mandatory is a key recommendation we issue in all the audits we conduct across the private, public and voluntary sector where large databases holding extensive datasets operate.

## 1.3 Alleged Illegal Access to Social Welfare Records

Issues with regard to INFOSYS were also identified as a result of a period of intensive engagement with the Department of Social Protection following the receipt of a breach report from the Department towards the end of 2010 indicating that suspicions had arisen regarding an employee's access to social welfare records. Thanks to the Department's technical ability to audit staff access to its systems in extensive detail, an internal investigation revealed that social welfare records were being accessed on a very large scale by the employee in question for no obvious reason. The Department of Social Protection's investigation led to the investigation and successful prosecution by this Office of a number of insurance companies who processed the illegally acquired data (see footnote 8 on page 88 of this report).

A criminal investigation is currently underway by An Garda Síochána with regard to this Department of Social Protection employee.

## 1.4 Who uses INFOSYS?

In the 2008 audit report of the Department of Social Protection it was noted

*There are a large number of external agencies who have access to INFOSYS.*

*FAS*
*Health Service Executive*

*South Dublin County Council*
*Fingal County Council*
*Dun Laoghaire/Rathdown County Council*
*Dublin City Council*

*Donegal Integrated Development Team*
*Department of Enterprise, Trade & Employment*

*Central Statistics Office*

*Department of Environment, Heritage & Local Govt. **

[12] ISTS (Integrated Short Term Schemes) is a claim administration system. ISTS users can view information and update specific data relating to short term schemes only depending on the level of access granted. ISTS account holders have access to INFOSYS via an option on the ISTS menu.

** Housing Rental Accommodation Sections in the County Councils not included in the above list may have a 'read only' limited snapshot of INFOSYS under an agreement with the Department of Environment, Heritage & Local Government.*
(p.36)[13]

Upon the commencement of the investigation into local authorities' use of INFOSYS it became evident that access to INFOSYS by local authorities outside of Dublin was not solely confined to Housing Rental Accommodation Sections. In February 2012, we queried this with the Department of Social Protection who responded

> "Some 30 local authorities have access to the Department's primary information system (INFOSYS). These accounts are required in connection with Rent Assessment, Homeless Unit and Housing generally."

In addition, within the Dublin local authorities, a far broader use than the uses originally envisaged became evident as the investigation progressed (see section 3 of this report).

## 1.5 Legal Basis for External Access to INFOSYS

### Legal Basis

Section 261 (1), (2) (3) of the Social Welfare (Consolidation) Act 2005 (see appendix 3) provides a legal basis for the request and exchange of data between the Department of Social Protection and other public bodies for the purposes of the 2005 Social Welfare Consolidation Act or for the control of schemes administered by the Department of Social Protection.

**SOCIAL WELFARE CONSOLIDATION ACT 2005**
**Exchange of information**

> **261.—**
> **(2)** Information held by the Minister for the purposes of this Act or the control of schemes administered by or on behalf of the Minister or the Department of Social Welfare may be transferred by the Minister to another Minister of the Government or a specified body, and information held by another Minister of the Government or a specified body which is required for the said purposes or the control of any such scheme administered by another Minister of the Government or a specified body may be transferred by that Minister of the Government or the specified body to the Minister.

Section 265 of the 2005 Act contains additional provisions for the sharing of information in terms of specific schemes such as payments under the Health Act, higher education grants and assessments or determinations made under the Housing Acts. Notably, section 265 refers to 'relevant purpose' as being required in order to legitimise such sharing with section 265 (3) stating

> A specified body may only seek information for the purposes of a transaction relating to a relevant purpose

We are aware that the provisions contained in sections 261 and 265 of the Social Welfare Consolidation Act 2005 are used extensively by specified bodies to request

[13] http://www.welfare.ie/EN/Topics/Documents/ODPCReport.pdf

and exchange information for the purposes of the control of schemes administered by another Minister of the Government or a specified body ("specified bodies" are defined in section 261(3) of the Act"[14]).

In terms of external access to INFOSYS, we accept that sections 261 and 265 of the 2005 Act provide a sufficient legal basis for these specified bodies to access INFOSYS on a 'read-only' basis in order to try and ensure that payments, grants and allowances are only made to those eligible to receive such assistance. The principle of 'relevant purpose' referred to in section 265 is equivalent to the 'purpose limitation' principle in data protection legislation. In 2010, we engaged with the Department of Social Protection 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 of Social Protection. The Guidelines[15] provide a basis for a general approach to data sharing within the public sector. Adherence to these principles should ensure that such data sharing is proportionate and in accordance with the Data Protection Acts.

### 1.6 Management and Hosting of INFOSYS

The INFOSYS database is currently managed and hosted internally by the Department of Social Protection.

Terms and conditions of usage are outlined in a 'Memorandum of Agreement' drawn up between the Department of Social Protection and all agencies authorised to use INFOSYS. The Department of Social Protection is ultimately responsible for INFOSYS but all entities authorised to access INFOSYS are also considered to be individual 'data controllers' in their own right.[16] This means that in terms of any external access, responsibility in relation to the legal use of the personal data on INFOSYS rests with the individual entities accessing the data.

## 2. INFOSYS INVESTIGATION

### 2.1 Conduct of Investigation

Initially, we commenced our investigation of INFOSYS by conducting a 'desk audit' which entailed extensive correspondence in the second and third quarter of 2011 with all external users of INFOSYS.

---

[14] **261.— (3)** In subsection (2) "a specified body" means a local authority (for the purposes of the Local Government Act, 1941), a health board, the Garda Síochána or any other body established—
(a) by or under any enactment (other than the Companies Acts, 1963 to 2005), or
(b) under the Companies Acts, 1963 to 2005, in pursuance of powers conferred by or under any other enactment, and financed wholly or partly by means of moneys provided or loans made or guaranteed, by a Minister of the Government or the issue of shares held by or on behalf of a Minister of the Government and a subsidiary of any such body.

[15] http://www.welfare.ie/EN/Topics/Documents/DataMatchingSummaryGuidelines.pdf
[16] http://www.dataprotection.ie/docs/Are_you_a_Data_Controller?/43.htm

## 2.2 Desk Audit

In May 2011, we wrote to the Department of Social Protection requesting that it supply the Office with a full list of accesses to INFOSYS in March 2011 by all external agencies granted access to INFOSYS. We outlined that the list supplied for each external agency should contain the usernames used to access the system, the time and date of the accesses and the specific records accessed, including the PPSN of the individual whose records were being looked up.

Arrangements were made with the Department of Social Protection for the secure provision of the data in question and the data was provided in June 2011. This information was to be used to identify access by each approved entity to INFOSYS and also to allow the INFOSYS Team to identify patterns of access and use by those authorised to use the system.

A list of the contact points utilised by the Department in dealing with the external bodies in relation to access to its systems was also provided to the INFOSYS Audit Team.

In July and August 2011, we formally wrote to each external body enclosing the listed accesses seeking the precise justification and purpose for each query conducted by its authorised users on INFOSYS during March 2011 (see appendix 1). Relevant policies and procedures and any staff guidance in relation to such access were also sought.

As detailed in the statistics below, 7 of the 37 organisations had to be contacted again in order to pursue matters further with them in the terms of the datasets and documentation provided as part of their initial response. (A sample of the warning letter issued is reproduced at appendix 2).

It was always our intention that the desk audit would be followed up as appropriate with targeted audits and physical inspections where issues of concern arose or to verify the information provided on foot of the exercise.

The desk audit produced a set of interim findings which then led us to engage with the Department of Social Protection and the large number of entities authorised to access INFOSYS in order to address the deficiencies identified as a result of the desk inspection.

**INFOSYS - Statistics**

| | | |
|---|---|---|
| How many agencies did we write to? | 37 | |
| How many received warning letters? | 7 | (19%) |
| How many did we arrange to physically visit? | 8 | (22%) |
| Number of external staff accesses in March 2011: | 55,000 | |
| Number of staff authorised to access INFOSYS in March 2011: | 705 | |
| Number of staff who accessed INFOSYS in March 2011: | 506 | |
| *[Number of staff authorised to access INFOSYS in March 2013:* | *527]* | |

# 3. LOCAL AUTHORITIES

## Usage of INFOSYS

The initial letter sent to local authorities authorised to access INFOSYS requested that each agency outline in their response:

i. the precise justification and purpose for each query conducted by your authorised users on INFOSYS during March 2011.

The first finding of note in terms of the local authority sector was the fact that several local authorities - Carlow, Kilkenny, Kildare, Westmeath and Tipperary North County Councils - did not appear to require access to INFOSYS as no user accounts had been set up with the Department of Social Protection. [17]

During the course of the investigation it also became apparent that two large local authorities did not as of February 2012 have an up-to-date memorandum of understanding in place with the Department to cover their use of INFOSYS. We indicated to the Department of Social Protection

> "We are surprised, therefore, that these bodies continue to have access to personal information held on the Department's systems in the absence of an agreement for them to do so."

Shortly after this revised memorandums of agreement were agreed and signed between these bodies and the Department of Social Protection.

Finally, the key finding for this aspect of the investigation related to the actual purposes for which INFOSYS was accessed by staff in local authorities. The majority of responses received from local authorities indicated that access to INFOSYS was confined to the Rental Accommodation Scheme Units in the Housing Departments of these authorities.

## 3.1 Rental Accommodation Scheme (RAS)

The Rental Accommodation Scheme (RAS) is a housing scheme under which individuals who have been receiving long-term rent supplement (in excess of 18 months) can apply to a local authority for long-term housing under the RAS scheme. RAS effectively allows successful applicants to transfer from the Rent Supplement (RS) to the Rental Accommodation Scheme (RAS). This nationwide scheme is in operation since 2005.

Under the RAS scheme, the local authority negotiates contracts with landlords for the use of their properties for medium to long term use whereby the council provide accommodation to those who have been in receipt of Rent Supplement for at least 18 months and who have a long term housing need which they cannot meet from their own resources. The tenant in return pays a rent 'differential' or contribution directly to the council based on household income.

[17] Since the investigation took place the Department of Social Protection has informed the Office that Kilkenny, Kildare, Westmeath and Tipperary North County have begun to use INFOSYS.

In order to apply for the scheme, initially applicants were required to complete a **RAS Housing Assessment Report Form** which the INFOSYS Team understood was a generic form, issued by the Department of Environment, Community and Local Government and in use throughout most local authorities.[18]
The Team noted that the final page of the Housing Assessment Report Form contained a declaration to be signed by the applicant(s) which stated:

> I/we declare that the information and particulars given by me/us above are correct and authorise the Housing Authority to make whatever enquiries it considers necessary to verify details.

'Fair Obtaining & Processing' is a fundamental principle of data protection and essentially means that an organisation collecting personal data must collect and use the information fairly[19]. We consider this wording to be too broad and does not provide the applicant with an indication of the type of checks being undertaken by the council. In particular, a check of the applicant's social welfare records as held on INFOSYS is not mentioned. We also note that this check is not mentioned in the Department of the Environment, Community and Local Government's explanatory leaflet on RAS[20]. Accordingly it is recommended that all Housing Assessment Report forms are amended to ensure that applicants are made fully aware of the type of checks being undertaken. This will need to be undertaken in conjunction with the Department of the Environment, Community and Local Government.

In total, the INFOSYS Investigative Team visited five local authorities (one inspection was part of a general audit of a local authority).

[18] Based on the June and July 2012 series of inspections this form has been replaced by another generic form – **Application for Social Housing Form** e.g. http://www.laois.ie/media/Media,7249,en.pdf

[19] 3.1 "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

[20] http://www.environ.ie/en/Publications/DevelopmentandHousing/Housing/FileDownLoad,2459,en.doc

**Case Study**

The INFOSYS Team visited Council X Offices in February 2012.

Council X indicated that prior to the commencement of the INFOSYS investigation in July 2011 other accesses to INFOSYS for queries within the Housing Unit may have taken place. However, on receipt of the July 2011 letter signalling the beginning of the INFOSYS investigation, Council X informed the Team that it had reviewed its policy and procedures and confirmed to the Team that INFOSYS is now confined to the RAS Unit in the Housing Dept of Council X. Council X also stated that the RAS Unit does not receive any requests from other areas within the Council for social welfare information held on INFOSYS.

A staff member working within the RAS Unit demonstrated to the Team in detail the nature of his duties in the RAS Unit. These duties centred predominantly on administering housing applications under the RAS scheme and using INFOSYS to confirm the amount and length of time a tenant is in receipt of rental supplement to ascertain whether they are eligible for RAS. It was confirmed to the Team that the RAS Unit also receives a quarterly report from the Dept of Environment, Community & Local Government providing details of all individuals within the geographical remit of region Y who may be eligible for RAS. The Team noted that these data feeds originate from the Supplementary Welfare Allowance Section of the Department of Social Protection and are supplied electronically to the Dept of Environment, Community & Local Government who in turn pass the feeds onto local authorities through a system developed and managed centrally by Dept of Environment, Community & Local Government. Access to the system using a unique password was demonstrated to the Team. Council X confirmed to the Team that it only receives data pertinent to Council X and not any neighbouring councils or other local authorities.

It was also indicated to the Team that the staff member would typically make frequent enquiries on INFOSYS to assist callers to the housing public counter in Council HQ who wished to check if they are RAS eligible. In the short period of time spent by the Team with the staff member, three enquiries were received from the public counter which would have required him to access INFOSYS.

The Team asked the staff member to enter on INFOSYS a number of the PPSNs for which Council X had not provided any usage justification in their written response. Some of the records checked were examined further by the Team and various scenarios discussed for each record accessed. Based on the various circumstances of the individuals in the records reviewed, the Team determined that the records of individuals looked up on RAS were plausible candidates for RAS.

The Team concluded that there was no evidence of inappropriate access in the RAS Unit of Council X on the basis of the information conveyed to the Team during the course of the inspection.

- It was recommended by the Team that every access to INFOSYS that could not be backed up by a RAS scheme application or linked with data recorded on an in-house RAS interview spreadsheet would need to be recorded on an INFOSYS ‘look-up’ query register to be maintained by Council X.

*[Since the INFOSYS investigation concluded, the Department of Social Protection has clarified to this Office that this data feed is still being supplied to the Department of the Environment, Community & Local Government from the Supplementary Welfare Allowance Section of the Department.]*

## 3.2 Access to INFOSYS for housing purposes other than RAS

Based on the uses highlighted in the various memoranda of agreement and the five physical inspections conducted on site, the INFOSYS Team concluded that some of the larger local authorities use INFOSYS across their Housing Units for the administration of a range of other housing schemes and services outside of RAS. This wider usage by urban local authorities was indicated in the 2008 audit of the Department of Social Protection – see p.93 above).

These purposes included:

**Rent Arrears**
A common reason aside from the Rental Accommodation Scheme cited by some local authorities as a reason for the checking of INFOSYS was in situations where rent arrears had been incurred by local authority tenants. These local authorities outlined their view that the calculation of repayment terms based on information sourced on INFOSYS was done to assist a housing officer to more accurately take into account the economic and employment circumstances of the tenants experiencing difficulties paying their rent.

**Rent Reviews.**
In one local authority visited, the Team came across a file which demonstrated how in the context of a rent review, the housing unit had checked INFOSYS to see if a tenant's spouse was currently working or receiving benefit as no income had been declared for her. They found that the declaration was correct and that she had no income. In addition it was noted that she had not been working for all of the previous year so in fact she would be entitled to a rebate on the rent differential paid by this household.

In several local authorities visited, the Team noted the uses of INFOSYS were even far more wide-ranging. Some of these uses had even been captured in a recently updated memorandum of agreement signed between one particular local authority and the Department of Social Protection in February 2012. Here, uses of INFOSYS by one particular local authority were listed as

(b) **Estate Management' purposes including**

- The prevention of fraud of both the housing and social welfare system
- Investigation of complaints of subletting Council units
- Investigation and prevention of duplication of tenancies (within the county and throughout the country)
- Investigation of breaches of excluding orders
- Establishment of who is residing in a property for investigations of alleged cases of ant-social behaviour

(e) **Allocations of Housing of Council owned and leased properties'**

- Confirmation of child benefit details
- Confirmation of income details
- Confirmation of relationship details
- Confirmation of current addresses as well as previous addresses

(k) **Homeless Service-**

- Confirmation of last and current addresses
- Relationship details
- Confirm payment types
- Confirming PPS Numbers
- To check if client has been granted rent allowance to confirm if he/she has moved so we can offer Support to Live independently
- Prevention of fraud

The Team examined some files which reflected the uses outlined in this particular memorandum of agreement. The local authority referred to its large stock of social housing units and indicated that INFOSYS is used to determine eligibility for housing in the first instance and to review rents at regular intervals (at least every two years). The local authority outlined that rent on council units is based on the individual's ability to pay and that Department of Social Protection income information on INFOSYS was essential in calculating differential rents and for carrying out rent reviews.

A sample of the files examined indicated that INFOSYS is used frequently by the Housing Unit for fraud prevention purposes, for example to ensure that the number of people resident in a local authority dwelling hasn't changed. The local authority demonstrated to the Team a particularly prevalent example of such a scenario where there is a single parent in receipt of housing on a certain rent differential who does not report a change in their circumstances such as a partner moving in. It was explained to the Team that if a single parent who is a local authority tenant wishes to live with their partner, that partner has to apply to the local authority for 'permission to reside' and if this is granted a new rent differential will be calculated based on the partners earnings also. The local authority indicated that it liaises with the Dept of Social Protection's anti-fraud unit and Council and DSP inspectors sometimes carry out joint visits to premises to ascertain who is actually resident there at a certain point in time.

*[Similar practices were encountered in the Team's other inspections of local authorities, particularly in relation to partners moving in without 'permission to reside' and the need to engage with the tenant as well as begin an exchange with the Department of Social Protection regarding the partner].*

The Team acknowledged the legal basis underpinning such exchanges of information and joint investigations. In particular section 15(2) of the Housing (Miscellaneous Provisions) Act, 1997 (see appendix 4) highlights a local authority's right to seek information from named bodies "in relation to any person seeking a house from the authority or residing or proposing to reside at a house provided by the authority or whom the authority considers may be or may have been engaged in anti-social behaviour" and its right of refusal to provide housing on grounds of failure to provide relevant information (as well as anti-social behaviour grounds).

Also, the Social Welfare Consolidation Act 2005 facilitates the request and exchange of information with another housing authority, the Criminal Assets Bureau, An Garda Síochána, the Minister for Social Protection, the Health Service Executive or an approved housing body in relation to occupants or prospective occupants of, or

applicants for, local authority housing. Nevertheless, this usage of INFOSYS was not in line with the understanding of the INFOSYS Investigation Team who had believed up until the investigation commenced that INFOSYS was only accessed within the RAS Unit of local authorities. The Team noted the wide uses of INFOSYS across the local authority's housing division and the access to detailed information by housing officers regarding benefits and the overall means of a household in receipt of or applying for local authority housing services.

Some questionable uses of INFOSYS were encountered in the anti-social behaviour context. In one local authority, a register was maintained of all accesses to INFOSYS made for anti-social behaviour (ASB) purposes. The practice of logging all such requests formally was commended by the Team. However, when the Investigations Team examined the logs for access to INFOSYS for ASB purposes it was noted that one of the entries referred to a man whom a tenant had reported as using a vacant house in their area to engage in child sexual abuse. The name of the individual had been supplied by a local authority tenant to the Anti-Social Behaviour Unit and the ASB Unit had looked up the name of the individual on INFOSYS and learned that the same man was a resident of the estate where the vacant house was situated. The Anti-Social Behaviour Unit indicated that it then passed this information verbally to social workers employed by the local authority who were physically situated in the same building as the anti-social behaviour unit. The Housing Unit was not able to provide an account to the ODPC as to what happened to this information subsequently.

The Team noted the entry in the register of access stated

> "Complaint received re alleged child abuse, social workers needed address to report this to the child protection unit"

Under the principle of 'purpose limitation' as set out in section 2(1)(c)(i) of the Data Protection Acts 1988 and 2003, there must be specific, clear and legitimate purposes for collecting personal data. The personal data sought and kept by data controllers should be sufficient to enable them to achieve their stated purposes and no more. The specific issue for this Office with the use of INFOSYS in the instances outlined above as captured in the memorandum of agreement is that data obtained for one stated purpose was being utilised for purposes potentially going beyond the purpose for which access to INFOSYS was granted despite the positive motivation for this use.

Also, the provision by the Department of Social Protection of access to INFOSYS to an external agency for a specified set of purposes is in itself an action that requires close monitoring in terms of any temptation on the part of other divisions in the agency not permitted to access INFOSYS to make requests to the unit with access.

In the same local authority, the Anti-Social Behaviour log referred to a female who had been in prison for anti-social behaviour and who was very vague to the council regarding the whereabouts of her son, also an offender. The council stated that the likelihood of this son taking up residence with this housing applicant would be a key determinant in the council deciding where and indeed whether to house her, so the local authority did run a check on INFOSYS to ascertain the latest whereabouts of her son.

Notwithstanding the provisions contained within section 15(2) of the Housing (Miscellaneous Provisions) Act, 1997, it is recommended that a register of all accesses to INFOSYS for anti-social behaviour or estate management purposes

should be maintained in local authorities in order to demonstrate the relevant purposes of all such accesses. In the instance outlined above, the local authority did maintain a register and this is to be commended.

An even wider usage of INFOSYS was encountered outside of the Housing Units in some local authorities.

- One local authority conducted a review of all existing domestic waste collection waivers and reduced the numbers eligible by almost half as a result of means-checking of recipients of the waiver on INFOSYS. This local authority no longer provides a domestic waste collection service.

We consider that this use of INFOSYS gives rises to issues related to the data protection principle of 'purpose limitation' given our understanding that INFOSYS was only to be made available to local authorities for housing related purposes. It is noted however that this purpose was outlined in the expanded Memorandum of Use signed between this particular local authority and the Dept of Social Protection in February 2012. *[SDCC confirmed to the Team that INFOSYS is no longer used for this purpose.]*

The use of INFOSYS for 'Public Liability Claims' was noted in the expanded memorandum of agreement signed in February 2012 between one local authority and the Department of Social Protection. Even though this possible use is captured in the memorandum, the local authority stated that INFOSYS is not currently used by the section dealing with Public Liability Claims. The local authority confirmed the Public Liability Claims section is also a registered user of **Insurance Link** (an insurance sector claims database subscribed to by some local authorities). We consider this gives rise to issues related to the principle of purpose limitation and such use should not be instigated. In addition, all reference to this proposed use should be removed from the memorandum of agreement between the local authority and DSP. *[The Department of Social Protection has since indicated its agreement with the position of this Office and confirmed it will be removed from the Memorandum of Agreement.]*

Finally, another use of INFOSYS that was not encountered in other local authorities but was again provided for in the memorandum of agreement was the use of INFOSYS in the Higher Education Grants Unit of a local authority to check the veracity of statements made by grant applicants in relation to their financial means. We indicated to this local authority that this did not appear to be a widespread use in other local authorities and the local authority stated that they considered it to be more efficient than asking the applicant to seek additional documentation from DSP in support of their application. However, due to the planned centralisation of the Student Support Schemes, it was indicated to the Team that this use would eventually be eliminated in a few years once the grant recipients finished their studies. We consider this practice again gives rises to issues related to the principle of purpose limitation.

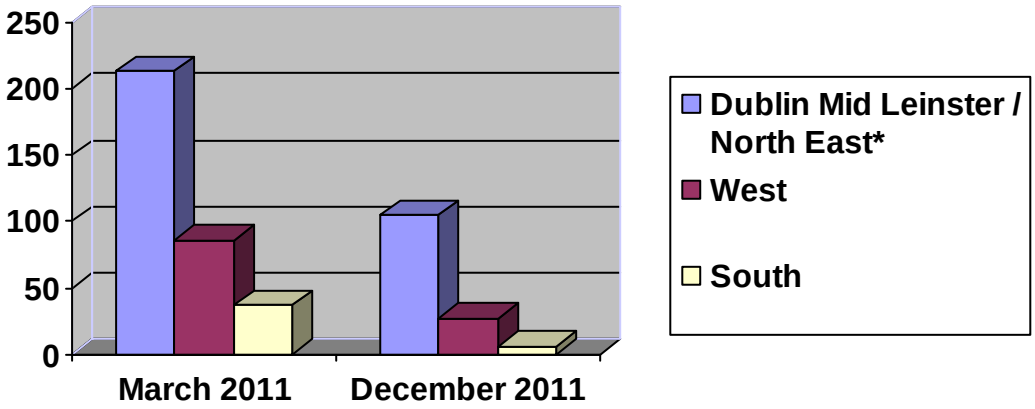
Similarly, another local authority indicated to us during the course of an INFOSYS inspection that although it had recently ceased to provide a domestic waste collection service, it was continuing to use INFOSYS as a means to collect arrears. The local authority outlined to the Team it considered this to be a worthwhile practice as they continue to receive arrears owing. We indicated that this use of INFOSYS needs to be examined in the context of the data protection principle of purpose limitation and retention.

As part of an audit of a local authority, (independent of the INFOSYS investigation) the Audit Team encountered a request to the Housing Section from the Environment section in the local authority seeking the address of an individual who the Environment section wished to issue with a litter fine. At the time, the Team indicated to the local authority that this request went beyond the purposes for which access had been granted to the Housing Division and referred it to section 2(1)(c)(i) of the Data Protection Acts 1988 & 2003. However, the Team noted that as the local authority was in fact the prosecuting authority under the Litter Pollution Act of 1997 that it could likely have sought to access this data legitimately via the Department of Social Protection had it cited 8(1)b of the Data Protection Acts.

## 4. HSE

Based on the user logs and account details provided by the Department of Social Protection, there were 336 INFOSYS user accounts across the HSE in March 2011 in comparison to 138 in December 2011. This equates to a 59% reduction in the number of user accounts. The INFOSYS Team noted a corresponding drop of 56% in the volume of accesses to the system when comparing the two periods.

**INFOSYS user numbers in HSE - March 2011 and December 2011**




***Combined totals for Dublin Mid Leinster and Dublin North East Region due to crossover of staff between the two regions**

The Team learned that this sharp decline in usage could be attributed to two key factors. Following the transfer of Community Welfare Officers from the HSE to the Department of Social Protection at the end of 2011, the overall number of authorised users drawn from within the HSE dropped significantly. Another key factor in the reduction in accesses in regional HSE divisions was the transfer of the medical card application process to the HSE's Primary Care Reimbursement Scheme (PCRS) in July 2011. This move was in line with a government decision to physically centralise the medical card application process on a national level resulting in all medical card applications and renewals being handled by the HSE's Primary Care Reimbursement Scheme situated in the HSE North East region in Finglas.

*[The number of authorised users within the Primary Care Reimbursement Scheme (PCRS) has increased since the INFOSYS investigation was completed with 98 authorised users as of March 2013. Overall the total number of HSE staff with user accounts for INFOSYS as of the 04.04.2013 is 252.]*

In terms of the overall purpose and uses of INFOSYS within the HSE, a single Memorandum of Understanding (MOU) for all of the HSE dated 29/04/2010 was supplied to the Team and the purposes for which INFOSYS is accessed were listed as:

- Blind welfare allowance
- Domiciliary care allowance
- Dental schemes
- Drugs payment scheme
- European Health Insurance Card (EHIC)
- GP visit card
- Home help service
- Immunisation services
- Inpatient services
- Institutional assistances services
- Long term illness scheme
- Maternity cash grant
- Medical care scheme
- mobility allowance
- motorised transport grant
- nursing home support scheme / fair deal
- ophthalmic & aural services
- outpatient services
- primary medical certificate
- supplementary welfare allowance

*[The INFOSYS Team noted that this agreement had since lapsed. The Department of Social Protection has since indicated that a new agreement is currently being drawn up with the HSE]*

The Team was informed that the medical card application process was the first to be centralised to the HSE's Primary Care Reimbursement Service (PCRS) and the following schemes would also be centralised on a rolling basis and in this order:

- Drugs Payment Scheme
- Long Term Illness
- Hepatitis C Scheme
- High Tech Drugs Scheme

In the course of investigating the processing of card applications by the HSE, the Team noted an unusual system for verifying home addresses through access to INFOSYS. The system involved the transfer of applications for such verification from one HSE location to another even though the original location itself had extensive access to INFOSYS. The Team pointed to the security risks associated with this system, including the increased risk of unsupervised access for non-official purposes to INFOSYS and the loss of data in transit. The HSE agreed to review the system in the light of the Team's comments.

Finally, one other example of the use of INFOSYS within the HSE South observed by the Team was the requirement by HSE staff to access INFOSYS in order to ascertain the correct PPSN of applicants for various HSE schemes and services.

HSE South showed the Team a list of clients who had applied for the long term illness scheme. It was indicated to the Team that they had received this list via an email from a Local Health Office with a request that the PPSNs be verified.

The Team concluded that the failure of applicants for all types of schemes to supply a correct PPSN appears to be a significant issue based on the data correction processes outlined by the HSE.

The Team noted in all the HSE offices visited that HSE users had only access to certain high level information on INFOSYS and that users could not for, example, access the income details of a client.

# 5. State Agencies

## 5.1 Central Statistics Office (C.S.O).

The **Survey on Income and Living Conditions (SILC)** is an annual survey conducted by the Central Statistics Office (CSO) to obtain information on the income and living conditions of different types of households. The survey also collects information on poverty and social exclusion. A representative random sample of households throughout the country is approached to provide the required information. The survey is voluntary from a respondent's perspective and nobody can be compelled to co-operate. The information is published in November each year in aggregate form and includes items such as the Poverty and Deprivation Indices, which are supplied by CSO to the Office for Social Inclusion in the Department of Social Protection.

Access to INFOSYS by statisticians working within the C.S.O is used to verify the accuracy of the data that has been gathered from the respondents to the survey via the PPSNs provided by respondents. It is important to clarify in this report that the checking of INFOSYS by the C.S.O. is conducted for statistical purposes only and unlike other agencies that may conduct investigations for anti-fraud and other permitted purposes, the C.S.O.'s terms of use is strictly confined to verification of the data to ensure the statistical integrity of the Survey on Income and Living Conditions (SILC). The CSO indicated in its initial response to this Office that Ireland is required to collate and provide this information for EU SILC statistical data processing purposes pursuant to Regulation (EC) No 1177/2003.

The INFOSYS Audit Team initially wrote to the CSO in July 2011. Later that month, the Team received a copy from the C.S.O. of the formal Memorandum of Agreement permitting access to INFOSYS and was provided with a copy of instructions for using INFOSYS issued to staff, in addition to a **SILC Users Confidentiality Protocol**.

The Team noted the **SILC Users Confidentiality Protocol** contained a very comprehensive set of procedures within the document to "guard against unintentional or otherwise disclosure(s) of information and to safeguard the confidentiality of data."

In particular the following instructions were noted and are to be commended in terms of their unequivocal clarity

- When browsing the INFOSYS system SILC staff should under no circumstances search/back search for records relating to family, relatives or friends. Indeed in cases where a member of SILC is data processing and comes across the details of relatives or friends etc, it would be best practice to refer such cases to another member of SILC staff for data processing. Further to this, SILC staff should under no circumstances access or browse information relating to themselves, a spouse or child(ren) or other persons known to them other than respondents that take part in the SILC Survey.

- When browsing the INFOSYS system SILC staff should under no circumstances search/back search for records relating to public figures, people that are currently in the public domain, people in the news or people know to them or made known to them by a third party, other than in an official capacity and for statistical purposes.

## 5.2. National Employment Rights Agency (NERA)

Disclosure of information between the Department of Social Protection and NERA is specifically provided for in Section 38 of the Social Welfare Pensions Act 2007 and disclosure of information between the Revenue Commissioners and NERA is provided for in Section 1093A of the Taxes Consolidation Act 1997 (as amended).

The INFOSYS Audit Team initially wrote to NERA in July 2011. A number of exchanges ensued between the Office and NERA regarding March and December 2011 access logs to INFOSYS but the Office considered ultimately that it had not received sufficient explanations for individual logs by all users, as "do not recall" was entered against a number of logs. A visit to NERA was subsequently scheduled to examine the logs in more detail.

NERA has a Memorandum of Agreement (MOA) in place with the Department of Social Protection dated 28.05.12 (see appendix 1). The Team noted that this MOA was unsigned and replaced the previous MOA dated February 2009[21].The Team noted that the MoA viewed on the day of its visit to NERA allows for

1. Processing of employment permits under the Employment Permit Acts 2003 & 2006.
2. Undertaking statistical research relating to employment permit holders in order to inform future employment permit policy as provided for in Section 37 of the Employment Permits Acts 2006.
3. Enquiries, inspections and investigations undertaken by NERA in respect of compliance with the Employment Permit Acts 2003 and 2006.
4. Enforcement by NERA of Determinations of the EAT/Labour Court against employers at the request of employees.
5. Prosecutions by NERA in respect of employment rights offences.
6. Enquiries, Inspections and Investigations by NERA Inspection Services of Employment Rights Compliance.

[21] this MOA was sent out by DSP for signature in April 2012 and a signed version was received back in January 2013.

NERA selected some sample complaint files and demonstrated to the Team how INFOSYS was used to extract and verify personal information.

In the first complaint file, an employee of a fast food outlet complained she was not receiving the minimum wage, bank holiday pay and annual leave from her employer. The business name was entered into the ER (employer) screen on INFOSYS and the inspector was able to check if the employee name was on the employer's P35 return.

Another complaint was made to NERA that an individual was not registered as an employer. A business has 18 months in which to register as an employer. In this instance NERA looked up INFOSYS by the individual's surname and initial and found that they were not registered as an employer.

The Team noted that in NERA's original response of 7th September 2011, NERA supplied a schedule of those users who did not access the system during the period under investigation.

### 5.3 Citizens Information Centre (Donegal)

The Department of Social Protection outlined to the INFOSYS Investigation Team that access to INFOSYS was provided in this instance to the Citizens Information Centre in Donegal on the basis that the Donegal Citizens Information Centre is an integrated part of a cross-governmental supported project - the Donegal Integrated Services project - which provides government services on an integrated basis from a one stop location. The Department of Social Protection confirmed to the Team that a memorandum of agreement with Donegal CIC is in place and that 'read only' access to certain scheme related information on INFOSYS applies. The Department of Social Protection also stated that as part of the agreement, the usage of INFOSYS is monitored at least on an annual basis by DSP Management in the North West Region and an audit report is produced. Finally, a detailed manual record is maintained by Donegal CIC of all records accessed, purpose and action taken etc. This record forms part of the management review process.

## 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 Data Protection Acts 1988 & 2003

## 6.1 Individual User Accounts

Prior to the commencement of the INFOSYS investigation, the Office was informed by the Department of Social Protection (DSP) that it had designated point(s) of contact with each of the member organisations accessing INFOSYS. It was outlined that all contacts must liaise with DSP in relation to the setting up of individual user accounts and with regard to any technical issues. It was confirmed that new accounts can only be set up by DSP – external bodies cannot set up new users themselves (see appendix 4). This practice is to be commended.

All organisations signing up to use INFOSYS are pre-approved for membership by the Department of Social Protection. Specific conditions of usage are outlined in a Memorandum of Agreement drawn up between the Department of Social Protection and each agency. All authorised users within each agency must also sign an agreement indicating they understand that access must be appropriate.

Specific procedures sometimes referred to as a "movers, leavers and joiners" policy should be in place in all organisations with access to personal data in order to increase or restrict previous access when a user 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. The INFOSYS Team examined these policies and procedures and considered that they must also 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 function.

We noted that technical mechanisms are in place on INFOSYS to identify redundant user accounts and that an automatic deletion of these accounts occurs for all accounts inactive for 120 days. In conjunction with this built-in-mechanism whereby an individual staff member's access to INFOSYS is automatically suspended after a certain period of inactivity, we consider that the designated point of contact for each agency authorised to use INFOSYS should also run a quarterly report, detailing all users who have not accessed INFOSYS/have been suspended. Such a report would enable each agency to identify redundant users and ensure their accounts are permanently shut down by the Department of Social Protection.

As referred to in section 1.2 of this report, a key finding of the 2008 audit of the Department of Social Protection was the fact that all activity including read-only access to records viewed through INFOSYS is logged by the Department and a complete audit trail of all 'look-ups' is retrievable. This in-built audit trail functionality was crucial throughout the INFOSYS investigation.

Upon the conclusion of its investigation, we consider it is of paramount importance that the Department of Social Protection makes available a reporting tool to all agencies with access to personal data for which the Department is responsible to allow them to check on the appropriateness of all accesses made by individual user accounts. We expect that this tool would be made available as a matter of priority.

*[The Department of Social Protection has since informed the Office of its plans to introduce shortly a process whereby all external agencies with access to INFOSYS will be required to carry out monthly checks on system accesses by their staff – see p.121 below]*

However in the interim, it is recommended that each agency embarks upon a programme of pro-active monitoring of access within their organisation. All users of

INFOSYS should also be made aware of these random spot checks which can be made by management periodically and informed clearly of the consequences if inappropriate employee access to data held on INFOSYS is detected.

Finally, with regard to legal responsibilities, the Department of Social Protection is ultimately responsible for INFOSYS but all entities authorised to access INFOSYS are also 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 INFOSYS rests with the individual entities accessing the data.

## 6.2 'Need to know' Access to INFOSYS

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 the investigation of INFOSYS, a focus was placed on access levels and authorisation levels for each subscriber to INFOSYS and an examination was undertaken of all searches conducted on INFOSYS in March and December 2011 for any evidence of inappropriate employee access.

In terms of the actual type of access allowed to an individual user, we were satisfied at the conclusion of the investigation that this was set to an appropriate level (certain areas on INFOSYS such as income earned not available to most agencies) and individual staff members only had access to data which they required in order to perform their duties. The specific concern raised by us in terms of data security was that "the current levels of external access to INFOSYS would be excessive taking account of the 'need to know' access principle”. The Office therefore examined the extent of access levels to INFOSYS in terms of the numbers of authorised users in each agency.

All entities authorised to use INFOSYS were asked to provide the Office with:

> details of any discrepancy between the number of authorised users with access to INFOSYS and the number who actually used the database during March 2011. A detailed explanation and justification is required as to why any authorised users did not access the system during this period.

Agencies were then requested to provide to the INFOSYS Investigation Team

iii. a copy of the internal procedures in place for approving and removing authorised users from INFOSYS.

iv. a copy of the internal guidance/instructions available to authorised users of INFOSYS informing them of the circumstances when INFOSYS may be accessed

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

In response to the request for details on numbers of staff with access to INFOSYS, the investigation revealed that overall 705 users had been allocated access rights to INFOSYS but that "of these users, 199 of the registered user accounts were not used to access the database in March 2011."

In the case of the HSE West, there were 77 authorised users but over 31% did not use INFOSYS in March 2011. In the case of Dublin City Council which had 59 authorised users, 14 (24%) of its authorised users showed no activity. NERA had 73 authorised users and almost 30% did not access the system. These user statistics identified deficiencies in polices and procedures in so far as the agencies granted access had failed to monitor or review their user-provisioning policies thereby exposing their organisations to increased risk from a security perspective and data subjects to an unacceptable risk of inappropriate access to their data.

*[Since the INFOSYS investigation concluded, the Department of Social Protection informed this Office in February 2013 that following a review of all external INFOSYS accounts in 2012, the number has now been reduced to 527 accounts.]*

## 6.3. Inappropriate Employee Access

In the initial letter issued to external specified bodies granted access to INFOSYS, the Office outlined that it wished to ascertain

> "there is sufficient oversight to ensure that all access by authorised users is for authorised purposes".

All external users granted access to INFOSYS were asked to provide the Office with:

- a copy of the internal guidance/instructions available to users of INFOSYS informing them of the circumstances when INFOSYS may be accessed

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

The search logs for all searches conducted on INFOSYS in March 2011 were also supplied by this Office to each specified body via extracts transmitted securely by the Department of Social Protection in order to allow each agency conduct an examination of usage within their organisation and to assist them in detecting any evidence of inappropriate employee access. This purpose was also clearly outlined in the letters issued originally to all agencies using INFOSYS where it was stated amongst other objectives that

"this Office wishes to ascertain that:

…• access is not taking place to the data on INFOSYS for purposes beyond the purpose for which the access was granted in the first instance (see appendix 1)

In the first instance, many of the usage justifications cited by the specified bodies as part of their initial response did not contain a precise justification for each search conducted by every user and they had to be contacted to request a complete response. Even then, many of the responses contained general usage justifications such as "accessed for business purposes".

For example, more specific justifications such as "medical card review" or "all access in relation to the Drugs Payment Scheme" were cited by the HSE in their responses but these reasons would appear against every search made by a particular user and so it was not apparent to this Office whether an actual check had been conducted by line managers to ensure the access was for bona fide reasons. Some usage

justifications provided by the HSE were specific against each PPSN searched such as “checked ISTS for immunisation service to ensure address correct when sending appointment”. This was the level of detail sought by this Office in all usage justifications. HSE Dublin Mid-Leinster clarified to this Office in a letter issued in September 2012 that “the wording used in the emails sent to managers requesting that they carry out this task clearly stated that each query should be checked and the purpose of each query noted.” HSE Dublin Mid-Leinster also confirmed in the same letter that confirmation was sought from each manager that the accounts had been checked.

Of course it was not possible to verify even the most detailed justifications cited unless an actual check of INFOSYS was made to verify that the details accessed appeared in line with the purpose cited. It was this type of check that formed a central component of the physical inspections carried out by the INFOSYS Investigations Team. Also, there was some additional analysis of responses through checks undertaken by the Team on an INFOSYS user account set up temporarily by the Department of Social Protection. This user account has since been deleted.

In 2012, as phase 2 of the investigation commenced, the INFOSYS Team wrote to a significant proportion of the entities initially contacted, indicating it was now seeking usage justifications for a new set of logs (December 2011). This phase of the investigation was initiated in order to examine further the users whose previous usage justifications had been insufficient or too general in nature.

A detailed analysis of the data and usage justifications received subsequently by the Office confirmed the concerns of the Office with regard to inappropriate employee access. Verified cases of inappropriate access to INFOSYS in contravention of the Data Protection Acts 1988 & 2003 were identified in many of the agencies examined. Serious cases of concern were identified across a range of bodies authorised to use INFOSYS.

Several external agencies such as the CSO and NERA commendably conducted their own internal analysis of the initial datasets supplied and contacted us to inform the Investigations Team that having closely examined the data and conducted further detailed interviews with the relevant personnel, inappropriate access had been detected. In these instances, it was indicated that disciplinary action had already been instigated and was in hand. Both the CSO and NERA continued to update this Office and provided comprehensive information on all disciplinary measures and actions taken.

### 6.3.1 C.S.O.

In August 2011 the CSO wrote to this Office stating that with regard to all four users authorised to use INFOSYS it could “confirm that all queries by the CSO authorised users on the INFOSYS system during March 2011 were for official statistical purposes only”.

Similar to other responses where only general justifications were provided, it was the intention of this Office to revert to the CSO seeking precise justifications. In the interim however, the CSO contacted this Office in writing in September 2011 to inform the Office that the CSO itself had since revisited the March 2011 usage logs and requested that an internal audit team undertake a more detailed analysis of any searches on INFOSYS which could not be accounted for at the time of their

response to this Office. The INFOSYS Team noted the number of searches requiring re-examination only comprised a small percentage of the overall number of searches conducted in March 2011 (approx 7%). All other searches had been accounted for satisfactorily by a direct comparison with the details of the individuals participating in the EU SILC Survey file.

The CSO informed the Team that as a result of this internal review it had uncovered inappropriate access in the case of three of the four authorised users and indicated that a formal investigation under Stage 4 of the Civil Service Disciplinary Code (the highest level of escalation) had been initiated.

The result of the investigation led to a number of sanctions being imposed on the three individuals namely: suspension without pay for a period of two weeks; a reduction in pay by one increment; and non-eligibility for consideration for promotion in the CSO for a two year period of service.

The motivation for accessing the records was also addressed as part of the CSO's investigation and "pure curiousity" was deemed to be the chief reason for two of the individuals. Whilst curiosity was also a factor in the third individual's usage, a large proportion of their inappropriate accesses were related to a recent bereavement where the INFOSYS system was used to obtain addresses so that acknowledgement cards could be issued to people who had sent cards of sympathy (also referred to in section 6.3 below).

We were disappointed to learn of the inappropriate access to INFOSYS committed by three of the four authorised users for the CSO but nevertheless welcomed the swift action taken by the CSO to conduct its own internal review in the first place and to immediately inform this Office as soon as the abuses came to light. The CSO continued to provide the Office with further updates throughout their investigation and the penalties imposed on its staff are in the view of this Office indicative of the unequivocal stance adopted by the CSO to ensure abuses such as this do not occur again.

### 6.3.2 NERA

On October 13th 2011, NERA submitted precise justifications for the March 2011 logs and stated at the end of the email

> "The examination of the usage carried out has identified some instances of inappropriate access which was of a personal nature. The Department's disciplinary procedure will be invoked in respect of the users concerned, and all users will be reminded of their obligations in this regard. "

On 11 May 2012 NERA informed this Office in writing that it had issued an email on foot of the inappropriate access coming to light to all staff on 19 October 2011.

An analysis of the March 2011 logs conducted internally by this Office in January 2012 also singled out two users of particular interest. On the day of the inspection, the Team examined several logs as supplied by NERA with regard to March and December 2011 accesses. As well as the users listed above, this led to a concern regarding accesses made by another user.

As referred to below, two searches conducted by an inspector in NERA were the dates of birth searches of two female colleagues. The officer in response stated that

it was “the practice in the office to celebrate birthdays where they are known, and that he accessed the records of the two inspectors concerned in order to obtain their dates of birth for this purpose.”

NERA subsequently advised this office that where such instances of inappropriate access were detected “the Regional Manager for the office concerned was requested to issue the officer concerned with a verbal warning in line with the Department's Disciplinary Procedure set out in Section 5 of the Human Resources Management Handbook. Regional Managers were also referred to Circular 14/2006: Civil Service Disciplinary Code revised in accordance with the Civil Service Regulation (Amendment) Act 2005”.

### Examples of inappropriate access uncovered:

- A series of searches made by one employee in the C.S.O took place so that the staff member could obtain addresses of individuals to whom they wished to send mass cards on foot of a recent family bereavement.

  *[This breach was identified by the CSO themselves during the course of an internal review of access on foot of the INFOSYS exercise and we were immediately notified.]*

- A series of searches made by one employee in HSE Dublin-Mid Leinster conducted on 15th December 2012 were conducted so that the employee could obtain the addresses of individuals to send these individuals Christmas cards (allegedly for another colleague in the HSE).

- A series of searches made by one employee in the HSE South region were conducted of family and neighbours all in one particular locality.

- Two searches conducted by an inspector in NERA were date of birth searches of two female colleagues.

- One search conducted by a female NERA employee was a search of a male colleague’s wife. It subsequently came to light that the female employee had not actually conducted this search and that it was actually conducted by her male colleague who, using her password, had looked up his wife’s details.

## 6.4 Accessing records of relatives “with consent”

In many cases where inappropriate access was investigated, it was admitted by the employees after further questioning by management that the searches were of family members and friends.

- One search conducted by a NERA employee was purportedly to check his brother’s address so he could send him a birthday card and the same individual on the same day checked his sister’s address to check her disability benefit details on her behalf.

In two HSE offices visited, employees appeared to consider it justifiable to cite searches conducted on INFOSYS as being on behalf of relatives “with consent”. On meeting with HSE Dublin Mid-Leinster to discuss logs of accesses to INFOSYS, the

issue of searches for family and friends emerging as a pattern within the context of the INFOSYS investigation was raised by the Team and the HSE personnel present responded by stating that staff conducting such searches had indicated that these searches on INFOSYS for family and friends would have been performed "with the consent" of the data subject. This view was echoed on the ground in another inspection conducted within the same HSE region. The Team outlined that such practices were unacceptable as this is not the purpose for which the HSE had been provided with access to the INFOSYS system. HSE Dublin Mid-Leinster subsequently clarified in writing to this Office in September 2012:

> "The discovery of inappropriate use of INFOSYS during this investigation whereby staff members accessed accounts of family members with their consent is unquestionably considered as non-legitimate activity by the HSE."

Some examples of justifications for searches made on INFOSYS by these HSE employees include

- "family enquiry with consent" – employees searched social welfare records of their own spouses, sons, daughters and in one case their son's girlfriend.

- "enquiry on behalf of family friend with consent".

- "this PPSN belongs to a sister of a member of staff who was asked to look into her SW claim"

- "this PPSN belongs to a boyfriend of the sister of a member of staff".

- One HSE South member of staff conducted a disability check for her uncle – this was checked by this member of staff on twenty separate occasions during March 2011 as well as conducting a social welfare check for her sister in the same period.

In terms of these findings, it was noted by this Office that at no point in any of the written correspondence between this Office and the HSE regions during phase one of the INFOSYS investigations was there any reference made to searches being performed on INFOSYS on behalf of relatives and friends - "with consent". This practice only became apparent to this Office in May 2012 following an examination by the INFOSYS Investigation Team of the justifications provided in the second tranche of logs reviewed – the December 2011 logs. There was no explanation or reference to this practice in any of the covering letters accompanying the usage justifications submitted in May 2012.

We subsequently advised the HSE regions concerned that we considered the checking of friends and families on Department of Social Protection records to be completely unacceptable and as instances of inappropriate employee access that should be reported to this Office in order for them to be investigated as data breaches. In terms of the "with consent" justification we indicated that we considered the consent of the data subject would be extremely difficult for the HSE to stand over unless the relatives were contacted and asked directly to verify they had provided their consent. Even in these circumstances, this is not the purpose for which access to INFOSYS is provided to the HSE and we concluded that the handling of an enquiry by a HSE employee on INFOSYS of a relative or family friend should regardless of "consent" be conducted at all times by another HSE member of staff

who is an authorised user of INFOSYS. For example, an authorised user of INFOSYS in the HSE could handle a written query regarding medical card applications and eligibility on behalf of a staff member's relative as long as that user actually handles medical card applications and is authorised to use INFOSYS for that specific purpose. Such a query should be submitted in writing and signed by the individual making the query. In effect, this query would then be handled like any other query received in writing to that section within the HSE.

We also consider it is imperative that all external users of INFOSYS understand that an enquiry on INFOSYS concerning 'disability benefit' or 'burial expenses' is completely unacceptable as these are patently not HSE services. The terms and conditions under which the HSE were granted access by the Department of Social Protection are strictly confined to usage being for HSE related services and schemes.

### 6.5 Non-Reporting of Inappropriate Access

The INFOSYS Team conducted several physical inspections of HSE offices in two different regions and during the course of one of these inspections, inappropriate access by a number of users in the HSE Dublin Mid-Leinster was identified. Initially, when we came across the inappropriate access we considered that evidence of any inappropriate access had simply gone unnoticed and not been reported to management or acted upon in any way. It subsequently emerged that the HSE Dublin Mid-Leinster region had been aware of such accesses since May 2012 but did not refer to them in their written response of May 2012 or to raise these findings verbally with us in the course of two separate meetings. The fact that the HSE Dublin Mid-Leinster region appeared to have been aware of inappropriate access to social welfare data but did not ever refer to this until after the matter was raised remains a cause for concern.

We wrote to HSE Dublin Mid-Leinster in September 2012 highlighting the inappropriate accesses. HSE Dublin Mid-Leinster, responded in September 2012 stating

> "The previous information returned to the Office of the Data Protection Commissioner was factual and in direct response to the questions raised. I appreciate that this did not include the subsequent actions taken in response to very serious breaches uncovered or a clear unambiguous statement that this was unacceptable behaviour."

The INFOSYS Team finally received written clarification from HSE Dublin Mid-Leinster region that verbal warnings had in fact been issued to 6 members of staff and their access to INFOSYS had been removed.

In another HSE region - HSE South - "inappropriate search" was cited in 11 instances by a user accounting for their accesses to INFOSYS in March 2011 with another user admitting "inappropriate view" alongside a number of searches. A key concern of the Office was the lack of explanation or reference by this HSE region to the "inappropriate views" or "inappropriate searches" cited when providing its official response during the second tranche of the INFOSYS exercise which sought additional employee usage justifications for INFOSYS searches. In all of the responses to the initial letters issued and subsequent INFOSYS follow-up investigations, there was no comment or reference made regarding justifications cited against some of the search logs such as "inappropriate search" or

“inappropriate view”. The INFOSYS Team met with the HSE South in July 2012 to obtain a general overview of practices and levels of access by HSE South to INFOSYS. There was no reference made at this meeting to the justifications cited by some of its employees in the recent exercise. (In terms of the inspection of HSE South, the INFOSYS Team was satisfied that the accesses made by the sole remaining user account for INFOSYS in the HSE South were for legitimate business purposes).

Subsequent examinations of the logs of usage made by former HSE South users of INFOSYS in March and December 2011 led the INFOSYS Team to indentify inappropriate access.

No account was subsequently provided to the Team of any internal investigation, disciplinary hearings or actions. The INFOSYS Team resumed some more in-depth examinations of the logs before writing to the HSE South in September 2012 to present its preliminary findings and seek a formal account in writing. These communications contained the details of individual users of INFOSYS whose usage the Office believed required an internal review by that HSE region. The letter also informed HSE South that the Office had

> “conducted an inspection of another office in a different HSE region in August 2012 and during the course of one of these visits a brief discussion was held with the HSE region in question regarding searches for family and friends emerging as a pattern within the context of the INFOSYS investigation. It was indicated to the Team that searches for family and friends would have been performed with the consent of the data subject. The Team outlined that such practices were unacceptable. “

A written response was requested by the Office regarding searches conducted by specific former users of INFOSYS in HSE South. With regard to one user who had cited eleven inappropriate searches over a one month period (March 2011), the HSE South indicated they had interviewed this particular staff member who had stated to them

> “This happened over a year and a half ago and I do not remember the specifics of my searches. However, I do know I had family members who were in receipt of Social Welfare and/or making claims and there would have been searches in relation to them.”

The Office was surprised that the HSE South in its response did not appear to have re-examined these searches of family members and friends themselves and so the Office re-submitted the details of the eleven searches to the HSE South. All the searches were of individuals living in the Kilkenny area with three of the individuals sharing the same surname as the INFOSYS user. In light of this, the Office sought precise clarification in writing as to whether the user’s line manager had entered the description "inappropriate search" during the completion of the exercise in August 2011 and if so whether the line manager had examined or discussed further these inappropriate searches with the staff member or reported them to management seeking an account of any action taken in this regard. The Office also asked

> “did the HSE South not consider that the inappropriate searches identified would need to be reported as data breaches to the Office of the Data Protection Commissioner?”

A final response on the matter was received by the HSE South in December 2012 which outlined that the staff member's manager had in fact met with the INFOSYS user and questioned them regarding the searches identified as inappropriate. It was stated that the staff member was reprimanded and apologised but that "the matter was not pursued under our disciplinary policy." The identification of the inappropriate accesses seems not to have been reported any further up the management line. HSE South informed this Office that

> "these searches were not reported as data breaches to me as Data Controller either at the time or following their discovery as part of the INFOSYS investigation by your Office. Please confirm whether or not this action should now be taken."

Given the passage of time since the breaches occurred, the Office responded indicating it considered the matter to be closed in relation to those particular incidents but they would of course be referred to in this report.

Overall, in light of both engagements with the HSE, we concluded that there was no attempt made by the HSE to raise any findings with this Office or the Department of Social Protection which came to light as a result of the INFOSYS investigation. Indeed, the whole point of the INFOSYS investigation was to require agencies to examine search logs in order to identify inappropriate access by staff members (see appendix 1). It was not until this Office itself highlighted the users from the HSE's own log extracts and queried justifications indicating inappropriate searches or searches made on behalf of family or friends that the HSE Dublin Mid-Leinster confirmed in one instance that it had been aware of these breaches and had taken some action in this regard.

HSE Dublin Mid-Leinster advised us in September 2012 that the staff concerned were disciplined in the following manner (one investigation still ongoing at the time);

1. Access to INFOSYS was immediately revoked;
2. A verbal warning being issued with a note put on their Personnel File;
3. The staff member was made aware of the inappropriate use of INFOSYS and the seriousness of his/her actions;
4. Staff member advised that this inappropriate use was totally unacceptable and against the Agreement between DSP and HSE;
5. Individuals were warned that if he/she had a further occurrence of a similar nature of misuse of other ICT systems, the disciplinary process would be invoked with immediate effect.

*[In terms of the ongoing investigation referred to above the Office was informed by HSE Dublin Mid-Leinster in 2013 that its internal investigation had concluded and the staff member concerned had received a warning as per the HSE Disciplinary Policy. ]*

Since the INFOSYS investigation concluded the HSE has contacted this Office to inform it that a number of new and additional measures have been put in place to strengthen controls and the monitoring of INFOSYS usage. These measures include:-

- A **'Data Protection Undertaking'** form reviewed and signed by all INFOSYS users,
- All users have received training in:
  (a) Use of INFOSYS
  (b) Data Protection Acts 1988 & 2003 including principles therein;
- INFOSYS accounts have been updated and recoded with identification codes to four regions and a specific code for PCRS. This means that the HSE can easily identify the area the user belongs to;
- All inactive INFOSYS accounts have been indentified and withdrawn;
- A standard national form has been developed for new INFOSYS account applications, temporary closures (e.g. sick leave/maternity leave) and permanent closure of accounts;
- Revised user names and new passwords have been implemented;
- A draft standard operating procedure has been developed and is being finalised with the DSP;
- INFOSYS User manual has been reviewed and circulated to all approved/trained INFOSYS users;
- A standard training package including business process is being developed at present.

We wish to highlight to all agencies using INFOSYS that the Data Protection Commissioner approved a personal **Data Security Breach Code of Practice**[22] in July 2011 to help organisations to react appropriately when they become aware of breaches of security involving customer or employee personal information. We consider that it is important for organisations to understand that data breaches would include all instances of inappropriate employee access. Also, guidance[23] from the Department of Finance on data security advises all public sector departments and agencies to report data breaches immediately to this Office. This includes inappropriate employee access to databases which staff members are authorised to access solely for work purposes.

## 7. RECOMMENDATIONS

- The practice and purpose of checks on INFOSYS made by external agencies should be directly referenced on all scheme application forms which use INFOSYS. From a data protection perspective this will ensure the fair obtaining and processing requirement is met, also allowing data subjects to exercise their rights of access under section 4 of the Data Protection Acts.

- The handling of an enquiry on INFOSYS of a relative or family friend should regardless of "consent" not be conducted by a relative with access to INFOSYS. INFOSYS should never be accessed for personal reasons and this is the policy throughout the Department of Social Protection. All such enquiries must be made in writing, signed by the data subject making the enquiry and passed on to the relevant section where users are authorised to use INFOSYS for the specific purpose the enquiry is based upon.

[22] http://www.dataprotection.ie/docs/07/07/10_-_Data_Security_Breach_Code_of_Practice/1082.htm
[23] http://www.dataprotection.ie/documents/guidance/GuidanceFinance.pdf

- All instance of inappropriate employee access should be reported to both the Department of Social Protection and the Office of the Data Protection Commissioner as they are data breaches and as such should be handled accordingly.

- The Department of Social Protection should make available a reporting tool to all agencies with access to personal data for which the Department is responsible to allow them to check on the appropriateness of such access to individual user accounts.

  *[The Department of Social Protection has since informed the Office of its plans to introduce shortly a process whereby all external agencies with access to INFOSYS will be required to carry out monthly checks on system accesses by their staff. To facilitate this, the Department has developed a batch programme which will generate all accesses for the previous month. These will be furnished to the agencies concerned who will then conduct agreed % checks on data. Where inappropriate accesses are discovered, they must be reported immediately to DSP, who will take appropriate action. In serious cases, this could include the termination of access to INFOSYS for the agency concerned.*

  *These new procedures will shortly be piloted in three external agencies (Fingal County Council, CSO and HSE West). Subject to the success of this 'pilot', it is the Department's intention to roll this process out to all external agencies at the earliest opportunity.*

  *Finally, each agency will be required to 'sign-up' to the process and this will form part of their MoA].*

- In advance of being provided with the reporting tool, it is recommended that each agency instigate a programme of pro-active monitoring of all access within their organisation to INFOSYS by conducting frequent random checks of employees and assigned users by managers at a local level. All users of INFOSYS should be made aware of these random spot checks and the penalties if inappropriate employee access to data held on INFOSYS is detected. As soon as the reporting tool is provided by the Department of Social Protection to each external agency such monitoring can be formalised and conducted on a wider and more frequent scale.

- All users of INFOSYS should be made aware of random spot checks and the consequences for them if inappropriate employee access to data is detected. Severe disciplinary penalties should be put in place to deter inappropriate employee access in the first instance.

- The Department of Social Protection should critically review the purposes for which access to INFOSYS is permitted with a view to ensuring that access for such purposes is proportionate.

- Every organisation authorised to access INFOSYS should maintain a register of all requests for disclosure and information received and issued. All information received from or passed onto external bodies such as Revenue, Department of Social Protection and An Garda Síochána should be noted by each authorised agency.

- Consideration must be given to the different requirements of each type of user approved to use INFOSYS and their access privileges to personal data should fully reflect these requirements. The nature of access allowed to an individual user should be set and reviewed on a regular basis. Individual staff members should only have access to data which they require in order to perform their duties.

  *[The Department of Social Protection has since outlined that access levels on INFOSYS are granted on a user group basis. These user groups are based on a matrix derived from a study of all INFOSYS users (internal and external). Eighteen different user groups were created to cover all varying levels of access required both internal and external. For example, User Group 02 covers Local Authorities.]*

  All agencies using INFOSYS should put in place focused internal guidance/procedures clearly setting out the use and purposes of INFOSYS within their own organisations. They should clearly state when it is legitimate to access INFOSYS and when it is not.

- A training structure to draw attention to requirements under data protection legislation and INFOSYS specifically 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 with particular emphasis placed on the safeguarding of customer data and the importance of access for business purposes only.

  *[Both the Department of Social Protection and specified bodies have outlined proposed approaches to dealing with these training requirements which are a matter of continuing engagement with this Office]*

# 8. FINDINGS

The most striking outcome of the investigation was the number of incidents of inappropriate access identified during the course of the investigation. As well as the internal investigations and disciplinary proceedings instigated as a result of these discoveries, these findings demonstrate the absolute necessity for proactive and random regular checks of access to be conducted by the external agencies themselves.

Serious abuse was detected by the INFOSYS Investigations Team in terms of inappropriate employee access. Explanations eventually obtained by the Investigations Team for inappropriate views by users of INFOSYS ranged from the bizarre to the banal: from the posting of Christmas cards and Mass cards to the reason of nothing other than 'pure curiousity' being cited in cases where family, neighbours' and friends' records were accessed. In the case of family members, this was sometimes purportedly done on their behalf, with their consent. The INFOSYS investigation and this report clearly outlines that it is not acceptable to conduct searches on INFOSYS on behalf of family or friends irrespective of whether it is the organisation's database(s) or an external one such as INFOSYS. The explanation provided by staff within one HSE region upon initially meeting with them that these searches were done with "the consent" of the family member or friend was met with disbelief by the Investigations Team. In the first instance, proof of consent could only be verified by contacting the relatives themselves and no evidence was offered by

the HSE of any such contact. Even if consent was provided, this Office considers it is wholly inappropriate for a person connected to an individual to conduct such a search, particularly since the system being checked was not even a HSE database. The stipulations referred to in the C.S.O's SILC Confidentiality Protocol (see section 5.1) adequately reflect the views of this Office in this regard. The HSE has since indicated its agreement with this view.

Of paramount importance is the necessity for the Department of Social Protection to make available a reporting tool to all agencies with access to personal data for which the Department is responsible to allow them to check on the appropriateness of such access to individual user accounts. We expect that this tool would be made available as a matter of priority but in the interim it is recommended that each agency instigate a programme of pro-active monitoring of all access within their organisation to INFOSYS by conducting frequent random checks of employees and assigned users by managers at a local level. All users of INFOSYS should be made aware of these random spot checks and the penalties if inappropriate employee access to data held on INFOSYS is detected. As soon as the reporting tool is provided by the Department of Social Protection to each external agency such monitoring can be formalised and conducted on a wider and more frequent scale.

We consider there is a need for a much greater degree of transparency with regard to access to INFOSYS. The provision to third party external agencies of social welfare data containing 7.7 million records needs to be clearly referenced in all scheme application forms be they medical cards or housing applications or information concerning compliance with statutory requirements. In addition, the fact that labour inspectors examine social welfare databases to check the employment details of employees or employers is not a practice of which the general public would likely be aware. This is especially the case where the data in question is used to make decisions on individuals. From the perspective of the rights and freedoms of the data subject, the Office considered that the checking of data on INFOSYS was not sufficiently transparent. Also paramount is the need for the public to be aware of their right to obtain a copy of any data held about them on INFOSYS and to seek corrections where that is necessary.

As part of the investigation, a review was conducted of some of the specified bodies' scheme application forms. Overall, the Office did not consider that adequate reference was being made at application stage to the fact that an applicant's details may be checked against data held by the Department of Social Protection for a number of purposes, including fraud prevention purposes. The information on the majority of application forms reviewed by the INFOSYS Investigation Team was considered wholly insufficient in terms of informing an individual adequately as to all potential uses of their personal data. Where information was provided it could at best be termed as basic and not meeting the requirements of fair processing. All parties have since accepted that appropriate notification as to the use to be made of the data should be provided at application stage.

Going forward, the Office expects that any checks on 'INFOSYS' will be directly referenced on relevant documentation used by specified bodies. It should be abundantly clear to the applicant that the details provided in their application will be checked against social welfare data. The correct legal basis should also be cited in any such notices. We recommend that the existence and purpose of INFOSYS be directly referenced on all scheme application forms which use INFOSYS. From a data protection perspective this will ensure transparency in the purpose and use of the system, also allowing data subjects to exercise their rights of access under section 4 of the Data Protection Acts. It can be assumed that this increased

transparency would also serve the interests of all parties concerned as increased knowledge of the checks made on INFOSYS database can be expected to dissuade any person considering engaging in fraud.

Overall, we consider that every organisation authorised to access INFOSYS should maintain a register of all requests for disclosure and information received and issued. All requests for disclosure must be made in writing (or followed up in writing) with a copy of all correspondence issued and received kept on file.

As well as the inappropriate access encountered within the HSE, the Team considered there appeared to be inconsistency in terms of the management of schemes leading to the sending back and forth of incomplete forms between HSE local health offices and the HSE's Primary Care Reimbursement Service. In terms of local authorities, the principal finding noted was the wider usage in urban local authorities which had been agreed with the Department of Social Protection and was captured in the memoranda of agreements reviewed. This report provides clarification as to which uses of INFOSYS this Office considered to be outside the scope of the intended use of INFOSYS. Going forward, it is recommended that the Department of Social Protection should critically review the purposes for which access to INFOSYS is permitted with a view to ensuring that access for such purposes is always proportionate.

Finally, a key focus of this investigation was the access levels within each member organisation, taking account of the actual numbers of authorised users versus the usage and activity of these users of INFOSYS during March 2011. Comprehensive documentation outlining policy with regard to user provisioning and policies designed to safeguard against inappropriate employee access are fundamental in this regard.

## Appendix 1 Original letter issued to external agencies with access to INFOS – July/August 2011

External organisation X

I am writing to inform you that the Office of the Data Protection Commissioner is commencing an investigation into the use of and access to personal data held by the Department of Social Protection systems by external third parties (under the authorisation of the Department of Social Protection). 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".

In this respect, the Office of the Data Protection Commissioner is examining all external access to Department of Social Protection data (via its INFOSYS system) to ensure access to the information held on this database is in full compliance with the Data Protection Acts. In brief this Office wishes to ascertain that:

- the current level of access within your organisation to the Department of Social Protection systems is not excessive taking account of the 'need to know' access principle
- access is not taking place to the data on INFOSYS for purposes beyond the purpose for which the access was granted in the first instance
- there is sufficient oversight to ensure that all access by authorised users is for authorised purposes only

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 precise justification and purpose for each query conducted by your authorised users on INFOSYS during March 2011. The extract included in this e-mail provides details of the actual accesses that took place. This was provided by the Department to this Office at our request.

However, please note that justifications are only being sought for every query that is accompanied by a PPSN. To clarify, if there is a query appearing without a PPSN e.g.,

01-3-2011 15:58.34 X-USER-FI CLIENT_SEARCH_TDF

we are not seeking a justification or purpose for this type of query as the Department of Social Protection has indicated to us that this type of query log merely indicates navigation of key menus within INFOSYS.

Also, if the same PPSN appears in a connected string of searches on a given date within a certain time range, we are seeking a justification for the search of that particular PPSN and there is no need to justify each query associated with that same PPSN.

We are also seeking

ii. details of any discrepancy between the number of authorised users with access to INFOSYS and the number who actually used the database during March. A detailed explanation and justification is required as to why any authorised users did not access the system during this period. The extract included in this e-mail contains a list of authorised users within your organisation which we received from the Department of Social Protection. You will see from the data extracts in the folder supplied that any user with a 0KB size file would not appear to have used the system in March.

iii. a copy of the internal procedures in place for approving and removing authorised users from INFOSYS.

iv. a copy of the internal guidance/instructions available to authorised users of INFOSYS informing them of the circumstances when INFOSYS may be accessed

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

Please contact XY or ZX, Office of the Data Protection Commissioner at 057 868 4800 or 087 9XX1CVB so we can provide you with a password to open the extracts.

I would ask that you provide the information sought (e-mail or hardcopy) by 19 August 2011. All responses submitted electronically should be emailed:

to: xx@dataprotection
cc: yy@dataprotection.ie

I am to inform you that if your organisation 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 INFOSYS by all external third parties.

## Appendix 2 Sample Warning letter issued to 7 agencies with access to INFOS –

Ms/Mr.
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX

Dear X.,

As you are aware, an investigation is being undertaken by the Data Protection Commissioner into the use of and access to personal data held by the Department of Social Protection systems by external third parties (under the authorisation of the Department of Social Protection).

This Office is disappointed not to have received a response from you on this matter and I refer you again to our correspondence of x and x (both enclosed) and follow up email reminders dated x and x September.

If a response is not received by x 2011, the Data Protection Commissioner will serve an Information Notice on you (which is a legal notice) to obtain the information requested. You should be aware that details of Information Notices issued in this context are included in the Commissioner's annual report and they may be subject to reporting in the media when the annual report is published.

Yours sincerely,

_____

**Senior Compliance Officer**

## Appendix 3 – Social Welfare Consolidation Act 2005

## Sharing of information.

**265.—(1) In this section—**

"data controller" and "personal data" have the meanings given to them by section 1 of the Data Protection Act 1988 ;

"information" means any personal data or information extracted from that data, whether collected before or after 5 February 1999;

"relevant purpose" means—

(a) for the purposes of determining entitlement to or control of—

(i) benefit,

(ii) a service provided by or under sections 45 , 58 , 59 and 61 of the Health Act 1970 or regulations made thereunder,

(iii) a payment under section 44 (3) of the Health Act 1947 ,

(iv) an allowance under the Blind Persons Act 1920,

(v) a grant awarded in accordance with regulations made under section 2 (as amended by section 3 of the Local Authorities (Higher Education Grants) Act 1992 ) of the Local Authorities (Higher Education Grants) Act 1968 , or

(vi) legal aid awarded under the Civil Legal Aid Act 1995 ,

or

(b) for the purposes of—

(i) making an assessment in accordance with section 9 of the Housing Act 1988 ,

(ii) a letting in accordance with section 11 of the Housing Act 1988 ,

(iii) the determining of rent or other payment in accordance with section 58 of the Housing Act 1966, or the control thereof.

[1998 s14(1)] (2) A specified body holding information may share that information with another specified body who has a transaction with a natural person relating to a relevant purpose, where the specified body seeking the information provides the personal public service number of the person who is the subject of the transaction and satisfies the data controller of the specified body holding the information that the information requested is relevant to the transaction for that purpose between the person and the specified body seeking the information.

[1998 s14(1)] (3) A specified body may only seek information for the purposes of a transaction relating to a relevant purpose.

[1998 s14(1)] (4) Where information shared between one specified body and another is found to be inaccurate, the specified body on making the discovery shall confirm with the person the correct information and advise the other specified body of the amended information.

[1998 s14(1); 2000 s32(1)(d)] (5) A person who knowingly seeks or transfers any information held by a specified body relating to another by using that other's personal public service

number, other than where the seeking or transferring of information is provided for under this Act or any other enactment, is guilty of an offence.

**Appendix 4. INFOSYS ACCESS (EXTERNAL). APPLICATION FOR A NEW INFOSYS ACCOUNT**

**INFOSYS ACCESS (EXTERNAL)**
**APPLICATION FOR A NEW INFOSYS ACCOUNT**

| **Please insert X in appropriate boxes:** | | |
|---|---|---|
| **Name of Staff Member:** | **Phone Number:** | **E-Mail Address:** |
| **Organisation:** | **Location:** | **Section:** |
| **Type of access is required** | | |
| **New Account** | | |

1. **Please give a Brief Business Reason for the setting up of new account and provide a brief outline of what the staff member will use Infosys for:**

2. **Please specify access required:**

**NEW ACCOUNT ACCESS**

3. **Please confirm the following:**

**Has Data Protection Declaration being signed:** **YES:** ☐ **NO:** ☐
**(attached Data Protection Declaration should be signed and a copy retained by the officer)**

| **Officer Details** | | | |
|---|---|---|---|
| **Name:** | **Phone Number:** | **E-Mail Address:** | **Date:** |

**Please forward Template to: xx@welfare.ie**

**To Be Completed by Data Access**

| **Infosys Account :** | **Has been set up :**<br>**Date:** | **Increased access granted.**<br>**Date:** |
|---|---|---|
| **USERNAME:** | **PASSWORD:** | **USERNAME:** |

| **To:** | |
|---|---|

| **From:** | **Data Access Section :** | **Date:** |
|---|---|---|

## Appendix 5 - Section 15(2) of the Housing (Miscellaneous Provisions) Act, 1997

**Provision of information.**

**15.**—**(1)** In this section, ‘‘specified person’’ means any of the following, that is to say:
(*a*) the Criminal Assets Bureau;
(*b*) a member of the Garda Síochána;
(*c*) the Minister for Social Welfare;
(*d*) a health board; or
(*e*) a body approved of for the purposes of section 6 of the Housing (Miscellaneous Provisions) Act, 1992, (to be known and referred to in this section as ‘‘an approved body’’).

**(2)** A housing authority may, for the purposes of any of their functions under the *Housing Acts, 1966 to 1997,* request from another housing authority or a specified person, information in relation to any person seeking a house from the authority or residing or proposing to reside at a house provided by the authority or whom the authority considers may be or may have been engaged in anti-social behaviour and, notwithstanding anything contained in any enactment, such other housing authority or specified person may provide the information to the housing authority requesting it.

**(3)** A health board may, for the purposes of its functions under Chapter 11 of Part III of the Social Welfare (Consolidation) Act, 1993, request from a housing authority information in relation to any claimant for a payment to supplement the claimant’s income in respect of rent or mortgage interest or in relation to any person residing or proposing to reside with the claimant and, notwithstanding anything contained in any enactment, the housing authority may provide the information to the health board.

**(4)** An approved body may request from a housing authority information in relation to any person seeking accommodation from the body or residing or proposing to reside at accommodation provided by the body, and, notwithstanding anything contained in any enactment, the housing authority may provide the information to that body.