An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Data Protection in the Office of the Revenue Commissioners

Final Report of the Data Protection Commissioner

Table of Contents

Throughout this report, the abbreviation "Revenue" stands for "Office of the Revenue Commissioners" and "ODPC" stands for "Office of the Data Protection Commissioner"

EXECUTIVE SUMMARY

This is a report of an audit of Revenue carried out by the Office of the Data Protection Commissioner on a number of dates between November 2008 and May 2009.

Revenue was selected for audit in the light of its status as a major public sector holder of personal data on individuals. Much of this data is provided in circumstances where the individual has no choice but to supply this information, in accordance with taxation legislation, if they wish to make a declaration of income or apply for a tax credit or relief.

The Office of the Data Protection Commissioner acknowledged from the outset of the audit process the strong and extensive legal powers facilitating the capture and disclosure of information to Revenue as an entity. In addition, Section 8(b) of the Data Protection Acts 1988 & 2003 provides a broad set of exemptions regarding the processing of personal data for the assessment or collection of tax. Notwithstanding this, these exemptions are subject to a prejudice test in each case.

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

1. LEGAL BASIS FOR INSPECTION

Section 10(1A) of the Data Protection Acts 1988 & 2003 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".

Under this authority the Commissioner instructed that a series of on-site inspections of Revenue be conducted commencing in November 2008. An Inspection Team was selected consisting of Gary Davis, Deputy Commissioner, Eunice Delaney, Assistant Commissioner, John Rogers, Senior Compliance Officer and Alan O'Grady, Senior Compliance Officer. A letter issued by the Data Protection Commissioner was sent to the Chairman of Revenue on 23 October 2008 giving notice of the Office's intention to conduct a series of inspections.

The Team indicated to Revenue that attention would be focused on the following data protection principles:

- Fair obtaining and processing of personal data
- Ensuring data is kept for one or more specified, explicit and lawful purposes
- Disclosure/further processing/transfer of data
- Ensuring the data processed is adequate, relevant and not excessive
- Ensuring the data processed is accurate, complete and up-to-date
- Data Retention: ensuring personal data is kept for no longer than necessary
- Safety & Security of Data
- Access Requests

2. BACKGROUND

The main focus of a data protection audit is to identify improvements that may be needed to ensure that the requirements of the Data Protection Acts are fully observed at all times. In tandem with this objective, an audit is also designed to ascertain whether there are any discernible breaches of data protection legislation evident.

The ODPC has witnessed an increasing recognition on the part of public sector entities that proper handling of personal data is also a matter of good customer service. If customers cannot trust the State to treat their personal information with respect, they will be increasingly reluctant to part with such information.

The quality of data security and access methods to personal data within Government Departments and bodies generally has been an issue of concern to the Office of the Data Protection Commissioner for some time. Because of the nature of its work, Revenue holds extensive and detailed personal information about its customers. Revenue stated to the Office of the Data Protection Commissioner that it fully accepts it has a strong responsibility to ensure that this information is collected appropriately, is maintained securely and is to be used only for the purpose for which it was intended. Revenue acknowledged that it shares public concern regarding a number of breaches of data security in the public sector in recent years and, in light of these events, has been engaged in a significant review of data access management and control policies, practices and procedures. Revenue clarified for the Team that the review, while not yet complete, had served to highlight a number of points of attention that the organisation was committed to addressing in order to ensure that information security is enhanced to a level commensurate with the high level of importance attached to it by the organisation from the Chairman down. Revenue stated it is actively engaged in a programme of work to address any deficiencies. Revenue highlighted public statements made by it where assurance was given that it takes such responsibilities seriously and considers breaches of data protection to be an issue warranting the strongest response up to and including disciplinary sanction. Finally, Revenue pointed to its Customer Charter which commits to treating the information taxpayers give Revenue in confidence, ensuring that it won't be used or disclosed except as provided for by law.

From the outset of the audit process, Revenue identified specific areas where arrangements could be enhanced and improved, for example, the need to develop a

comprehensive data retention policy and devise enhanced activities on the data protection training front.

3. PRE-INSPECTION

Prior to the issue of the formal letter of intention to audit, ODPC representatives met with Revenue officials from Corporate Services Division (CSD) to discuss and assess the scope of the proposed audit. The initial stages of the Revenue audit programme were focused on obtaining an overview of the organisation in terms of the capture and movement of personal data within it. This initial exploratory stage allowed the audit team to identify priority areas, systems and processes for inspection. Advance documentation was sought in relation to data flows and system architecture within Revenue as well as details of the legal basis for any third party data transfers out of Revenue.

The Team outlined the purpose of the inspection and explained that the main focus of the audit was to track the capture and movement of personal data through Revenue's systems and beyond. Another key objective of the inspection was to examine and assess the security measures taken to protect any personal data held by Revenue from unauthorised access, alteration, disclosure or destruction.

The areas and operating systems of Revenue selected for inspection were chosen at random, albeit, with a particular focus on those areas which were believed would be most illustrative of the physical and technical measures in place for the processing of personal data in Revenue.

4. THE INSPECTION

4.1 Introduction

An introductory meeting took place between officials from Revenue and the ODPC on 20 November 2008 to ascertain what areas of Revenue would likely be inspected in the course of the audit process. The Revenue Team was led by Norman Gillanders, Assistant Secretary, Operations Policy & Evaluation Division (OPED), and the OPDC Team was introduced to the following Revenue officials:

> Paddy Gleeson (Head of Data Protection for Revenue), Orna Maguire, Bart Felle[1] – Corporate Services Division (CSD)
> Gerry Howard, Michael Colgan, Brian Boland – Investigations & Prosecutions Division (IPD)
> Mary Hughes – Planning Division[2]
> Liam Ryan, John Barron, Vincent Duffy – Information & Communications Technology and Logistics Division (ICT&L)

[1] Formerly part of Strategic Planning Division (SPD) which was wound down in January 2009 and whose Branches were re-assigned into Corporate Services Division and Planning Division.
[2] In January 2009 Operational Policy and Evaluation Division (OPED) formed part of a new expanded Division 'Planning Division'.

Revenue Overview
The ODPC team were provided with an overview of Revenue. The organisation employs in the region of 6,500 fulltime equivalents or 7,000 people working at some 130 locations countrywide. Revenue is currently made up of 15 Divisions covering 7-8 significant taxheads. Around 1,100 staff work in PAYE areas.

Revenue's core business is the assessment and collection of taxes and duties. Revenue's mandate derives from obligations imposed by statute and by Government and as a result of Ireland's membership of the European Union. In broad terms its functions include –

- Assessing, collecting and managing taxes and duties that account for over 93% of Exchequer Revenue
- Administering the Customs regime for the control of imports and exports and collection of duties and levies on behalf of the EU
- Working in co-operation with other State Agencies in the fight against drugs and in other cross-Departmental initiatives
- Carrying out Agency work for other Departments such as the collection of PRSI for the Department of Social and Family Affairs
- Provision of advice on taxation issues.

A large amount of ongoing business involves dealing with some 2.2m taxpayers. Revenue informed the Team it had dealt with 940,000 personal callers in 2007 and currently handles 7,000 calls per day to its regionalised Lo-Call 1890 numbers. Revenue indicated to the Team that since the introduction of the Revenue Online Service, paper interactions with taxpayers are reducing. In 2008, 654,000 online payments were recorded.

Organisational Structure
Revenue explained to the Team that its structure is designed around its customer base. Revenue Regions are responsible for customers within their geographical area, except for large corporate bodies and high wealth individuals who are dealt with by Revenue's 'Large Cases Division'. Revenue also has policy, legislation and tax interpretation functions. The 15 Revenue Divisions referred to above are made up as follows:

- 4 Regional Divisions
- Large Cases Division
- Investigations and Prosecutions Division
- Customs Division
- 3 Revenue Legislation Service Divisions (Corporate Business & International Division, Income & Capital Taxes Division and Indirect Taxes Division)
- 2 National Office Divisions (Corporate Services Division and Planning Division)
- Revenue Solicitor's Office
- Information & Communications Technology and Logistics Division
- Collector-General's Division

ODPC Introduction
From the outset, the ODPC outlined its recognition that Revenue occupies a special position as a consequence of the broad exemptions that exist under Section 8(b) of the Data Protection Acts regarding the processing of personal data for the assessment or collection of tax. Nonetheless, the Team stressed that these exemptions are subject to a prejudice test in each case and Revenue is still required to meet all the other requirements of the Acts in terms of retention, disclosure and security. Revenue assured the Team that it understood these requirements and had invested major resources to ensure compliance with requirements under data protection legislation and to protect itself against any risk of non-compliance.

4.2 Inspection of Specific Divisions & Systems

4.2.1 Investigations and Prosecutions Division (IPD)

There are approximately 230 staff working in **Investigations and Prosecutions Division in** a number of locations in and around Dublin and a branch office in Co. Donegal. The Division covers 5 main work functions:

- To prosecute customs and tax offenders (over 500 per annum)
- To deal with customs seizures - firearms, diesel, cigarettes, etc.
- To investigate bogus non-resident accounts
- To liaise internationally on combating drug smuggling
- To liaise with the Criminal Assets Bureau

Revenue described information as integral to the operation of IPD in order to identify customs and tax offenders. Revenue stated to the Team that data is collected on foot of legislative provisions and court orders and that the IPD works closely with the Revenue Solicitor**'**s Office and the Director of Public Prosecutions. IPD has access to and collects the following different types of data:

- Intelligence data
- High Court Order data
- Compliant taxpayer data
- Data on bench warrant seizures
- Mutual assistance data via double taxation agreements etc. (international)

IPD outlined to the Team that it maintains close relationships with An Garda Síochána, the Police Service of Northern Ireland and UK Police. All exchanges of data were stated to be subject to appropriate protocols and handled by the competent authority in each jurisdiction.

Depending on the type of data available, IPD will make an assessment as to whether an individual is 'a tax risk' or not. Revenue stated this approach allowed it to concentrate its resources on priority cases.

Within the Investigations area, a user initially logs on to the system using a username and password. Depending on an individual's assignment, different levels of access to

local Revenue Systems were apparent. The particular logon examined by the Team (at Assistant Principal Officer level) provided access to the Integrated Business Intelligence Portal (IBI) (see also 4.2.4 below) using a further username/password. IBI then takes this user into the Investigations menu which, in turn, provides access to certain sub-menus such as Vehicle Registration Tax (VRT). Within VRT, vehicle and owner details are displayed, including PPSN. By clicking on PPSN, the user is provided with an overview of the vehicle owner's general tax details. The tax screens note previous interactions between the customer and Revenue and record the names of any officers who have made any amendments previously to the record.

The Investigations menu also provides information on the customer such as previous address, share details (if applicable), property details and risk summary (information taken from the REAP system - see 4.2.2 below).

From the user's desktop, icons for other systems are displayed. CNET (Customs Network) records details of customs seizures and declarations. Information on suspects is input by authorised officers based in customs areas such as Dublin Airport. CNET is a standalone system for Ireland with no connection with any other country. No access could be made from the desk inspected to either the BNR (Bogus Non Resident system) or CRPlus (Common Registration System) as they belong to other business areas.

The Team visited the Investigations Support area which examines and collates information received from regional offices or through telephone conversations and attempts to match this information against existing Revenue data. Third party information is sought in some cases, but in all cases Revenue specified that it must be specific, i.e., trawling exercises for information are not allowed. If there is considered to be a basis for a prosecution, the information is passed to the Criminal Investigation Unit. The Team was again provided with a view of a Principal Officer logon and noted that different accesses were available compared to the access observed in the Investigations Area. Here the CRPlus system was accessible by means of a badge swipe and username and the user had no logon to CNET.

Revenue outlined to the Team that all functions undertaken by this area are underpinned by the Taxes Consolidation Acts. In addition, the performance of some of the functions may require the approval of an Assistant Secretary, a Revenue Commissioner, or, in certain cases, a judge. From a data protection perspective, the Team outlined to Revenue that it must be in a position to demonstrate an appropriate legal basis for information collected in respect of one tax head to allow for it to be used in an investigation under another tax head. In response to this request for clarification, Revenue stated that Section 872 of the Taxes Consolidation Act applies. Section 872 of the Taxes Consolidation Act specifically provides that any information acquired by Revenue in relation to any tax or duty under their care or management may be used by them in connection with any other tax or duty for which they are responsible.

The Criminal Investigations area was examined in terms of the procedures in place for securing personal data. The secure storage area was examined and it was found that access was restricted to only those personnel with a business need to access it. A random sample of files was examined. The information contained in these files did

not give rise to any concerns in terms of the fair collection and processing of personal data. It was apparent however from an examination of the files that at present there is no retention policy in relation to the deletion of files which are no longer serving the purpose for which they were created. This issue will need to be addressed.

The Team also met with relevant Officers from the Drug Enforcement Section. Again the principal focus was to ensure that appropriate measures were in place for the security of personal data processed in this section. This section was segregated from the remainder of the already secure building with additional security in place.

Security
IPD's Dublin building is a shared facility. IPD shares this building with some colleagues from Revenue's Dublin Region and also with a small group of colleagues from Revenue's East and South East Region.

The Team noted there appeared to be a high level of security in place both within the building and at entry points. Cars entering the underground car park must have security clearance and are swiped to gain access. Steel shutters close off the car park at night. Access to the building is via the front door or from two entry points from the car park. All entry points have CCTV in operation, and have swipe card access. The front desk has 24 hour security.

Inside the building, all entry points to IPD offices require swipe card entry and exit. All swipes, including failed swipes, are logged. CCTV is in operation on all floors.

Within the Customs Investigations area manual files are held in steel cabinets – access is by swipe card. Older files are held on a separate floor and, again, the room requires a swipe card issued to authorised officers to enter and exit. The Inspection Team was able to see that officers not working in the area had any swipe attempt rejected. CCTV is in operation.

The communications room is accessible to 3-4 IT liaison staff and 3-4 service staff by swipe card (entry and exit). UPS (Uninterrupted Power Source) is in operation.

4.2.2 Planning Division

Revenue's Planning Division has a staff of 196 fulltime equivalents at present, working from a central office where it devises policies and programmes to support Revenue's operational Divisions and Regions. Its main role is to evolve operational policy within the organisation and report to the Board of the Revenue Commissioners. Day to day functions include:

- Monitoring Revenue's audit programme
- Dealing with Parliamentary Questions
- Forecasting and statistics
- Management of the Revenue Online Service (ROS)
- Monitoring of customer services
- Ensuring that Finance Bill changes are carried forward into Revenue systems
- Designing information leaflets for customers
- Driving Capital Taxes policies and programmes

- Compliance Policy
- Risk Evaluation Analysis and Profiling System (REAP)

Business Analytics

As part of its customer focus, Revenue stated to the Team that it uses business analysis in order to streamline and improve the provision of targeted customer service. A tool referred to by Revenue as 'Business Analytics' assists Revenue in a number of different ways:

- To identify customers who may be entitled to claim specific tax credits
- To develop a better understanding of its customer base
- To examine internal/external risks of fraud

Revenue demonstrated to the Team one particular analysis program undertaken to increase the rate of take-up for a specific tax credit by eligible PAYE taxpayers. In order to create analytical base tables (ABTs) of data, Planning Division liaised with ICT&L Division, who in turn extracted PAYE customer data, such as demographic variables, tax and income details, and tax credits claimed, from Revenue's data warehouse, which is essentially a store of all Revenue customer information. The created ABTs were made available on a dedicated server accessible to nominated staff in Planning Division. Planning Division used this data to build predictive models, carry out segmentation and query processes.

In the exercise to encourage eligible PAYE taxpayers to claim a specific tax credit a sample of 2,000 PAYE customers was taken. Revenue contacted these customers by post and encouraged them to claim their entitlements using a variety of channels. Revenue acknowledged that initial indications were that the increased uptake[3] among the 2,000 PAYE customers for the tax credit, as a result of their exercise, was low (around 1.5%). However, subsequent to the inspection Revenue has indicated that it undertook a further analysis a few months later which revealed that the uptake had increased to 5.5%. While this approach did increase the rate of take-up of the specific tax credit the Inspection Team was informed that there are no immediate plans to repeat this exercise.

Revenue indicated that the use of 'Business Analytics' could also provide information to Revenue on the profiles of its customer base. A segmentation model was developed on the PAYE customer's tax profile, i.e. their income, tax paid and credits claimed. This approach found 10 segments; these were then mapped onto demographic data and found to give good separation.

While Revenue indicated that customer segmentation and building predictive models are very new developments within the organisation and only at the planning stage, there may be scope, going forward, for its further development in relation to compliance issues and in identifying more suitable cases for audit. For example, current figures show that a specific proportion of cases that Revenue selects for audit

[3] The highest uptake per channel was from PAYE customers who completed a paper application form and responded by post, followed by on-line claimants and lastly those who contacted Revenue by phone to claim the specific tax credit.

produces a nil yield. There may be scope to decrease the number of nil yielding audits using these techniques.

Planning Division outlined how it also uses 'Business Analytics' tools to examine potential fraud issues by analysing the PAYE system. It was also demonstrated to the Inspection Team how 'peaks and troughs' in transactional data activities carried out by Revenue staff can be identified. For example, analysis can show the number of 'edits' made on an individual record over a specified period of time.

The Team pointed out a functionality available that allowed a staff member to print or email a particular screenshot without leaving a 'footprint' and recommended that the analysis be extended to cover read only access or 'look-ups'.

In this context, Revenue also commented that certain categories of customers who are prominent and in the public eye, are dealt with separately to mainstream PAYE customers and are handled by dedicated Districts/Units with access provided to certain authorised officers. The Team was informed that these categories are kept under constant review.

As mentioned above, data provided from the use of the 'Business Analytics' tool is held on a dedicated server located in Revenue's primary Data Centre in Dublin. Revenue clarified that only 6 staff members within Planning Division have access to the server by means of a specific logon. While visiting ICT&L in the primary Data Centre in Dublin the Inspection Team inspected the location of the server and examined the list of users set up with access to the server. There were no issues arising.

REAP

Revenue primarily uses the REAP system to evaluate customer tax risk. The REAP system analyses Revenue data and limited third party data secured by legislative means, allowing Revenue to select cases for intervention or audit. Essentially REAP is a tool which collates and interrogates customer data from within the Revenue data warehouse. The system allocates a score indicating the level of potential tax risk associated with a customer based on a series of business rules. Revenue's REAP Unit is located in Dublin with limited access available from each of the 4 Revenue Regions**.** All Revenue PC's have the REAP icon, but the REAP System is accessible only via the officer's identity and password. The officer's identity is cleared for access by the REAP Team following Regional Office approval. Revenue stated to the Team that REAP was piloted during 2005/6 and went live in 2007.

At present, Revenue remarked to the Team that REAP is primarily concerned with business customers – corporate and sole traders. Decisions on what areas or sectors are to be examined are made by Planning Division, though the Regions will also make recommendations on local areas that may be of interest to Revenue. However, given the present economic climate, Revenue indicated that the use of REAP may be extended to evaluate risk across the PAYE sector. This would involve REAP examining some 2.2 million cases. The focus of REAP on any PAYE application would be to look at additional assets a customer has, for example, anything under Capital Gains Tax, or if a customer is also involved in another additional business

activity, etc. Such persons may be liable for additional tax liabilities. Revenue stated that REAP would not link couples unless they had requested joint assessment.

Quarterly interrogations of the data warehouse focusing on business customers are undertaken using REAP. This interrogation, or risk run, involves the use of some 220 different rules or parameters. The Inspection Team viewed previous results, containing some 900,000 records, from the October 2008 risk run. Revenue demonstrated to the Team how analysis of these results can assist Revenue identify cases where intervention – audit - may be required. Revenue estimated that some 60% of all Revenue audits are based on the top 20% of 'risks' identified from the REAP risk run and analysis. Revenue stated that they also undertake random audits, although analysis of the audit function has identified that the audit targets selected using REAP show an overall lower level of compliance to those selected at random. The Team were informed that REAP results are based on an analysis of a maximum of 5 years of data for a customer. Therefore, the REAP rating of a customer may fluctuate as the oldest year is dropped from the data and the current year is added to the analysis.

Revenue then outlined to the Team the different levels of access to REAP and the different tools deployed within REAP.

Demonstrations were given to the Team, in both the Central REAP Unit in Dublin and in the Galway Regional Office, of how REAP analysis is undertaken. By accessing REAP through the Case Select Tool, a list of the 'riskiest' cases (top 20%) in a particular category can be produced and, if appropriate, selected for audit. For example, using the Case Select Tool, an officer can apply local analysis parameters to create sectoral projects, e.g. a list of fast food outlets with high profit margins within a particular regional area. Cases can be selected in this way by using the appropriate NACE code (an EU wide code used to designate organisation type). The results produced by Case Select list businesses and sole traders based on the parameters entered, with entries flagged where a case is currently being audited or if a prosecution is ongoing.

The Case Select Tool is available via a desktop icon and alpha/numeric logon to designated Selection Managers only. Selection Managers select the cases for possible audit and cases are then assigned within the system by the Selection Manager to members of his/her audit team. There are around 120 Selection Managers authorised across the 4 Regions. Selection Managers are, in the main, confined to officers at Assistant Principal grade and above. Some officers at Higher Executive Officer grade have access and for these officers an individual business case would have been made by their managers. Access to the Case Select Tool is granted by way of the AIM Security Tool. Revenue stated to the Team that a designated officer in Revenue's Four Regional Offices will nominate officers whom they are satisfied qualify and require access to Case Select.

Revenue's Central REAP Unit in Dublin then examine the relevant business cases and make the final decision to either grant or refuse access. The Case Select Security Document states that

> "A twice yearly review will be conducted by the REAP unit of the list of all officers with access to Case Select. Any Officer who has transferred, changed responsibilities or who has not accessed Case Select within the previous 6 months will have their access rights revoked."

In addition, the Team were informed that non-usage of the system by officers who have access rights is also closely monitored at a central level. Revenue elaborated on this by explaining that the Central Reap Unit has in the past removed access where no usage of the system occurred. Furthermore Revenue informed the Team that the twice yearly review produces lists pinpointing low usage which are circulated to Regional Offices to confirm whether access is still required.

The Inspection Team noted that the Case Select Tool automatically locked the user out after several minutes when the screen was left inactive.

Once the Selection Manager has assigned a set of possible cases to officers, a tool referred to by Revenue as the Risk Profile Viewer allows these officers who conduct Revenue audits to view and prioritise these cases for audit. The Risk Profile Viewer provides detailed information on issues surrounding a case and the years in which the issues arise. The Risk Profile Viewer has a link to the Integrated Business Intelligence system (IBI) which provides the auditor with a comprehensive view of the customer, including information on categories such as Vehicle Registration Tax and Suspicious Transactions Reports (See section 4.2.4 below for further information on IBI).

The cases screened by the auditor are then submitted to the Selection Manager for approval and final assignment for audit. Once a case has been assigned to an auditor, an initial letter of intention to undertake an audit is issued to the customer. The letter is also issued to the customer's listed business accountant. Depending on the type of audit to be carried out, action may range from a desk-based audit (usually in the case of a single tax head audit) involving correspondence with the customer seeking specific information, to a full on-site inspection (comprehensive audit).

The Audit Case Management tool provides details of correspondence and actions taken in the course of the audit, including the final outcome. An auditor can see only those cases which have been assigned to him/her. Revenue clarified for the Team that all access by auditors to the Case Management Tool is logged.

Arising out of an audit, Revenue publishes (as provided for under the Taxes Consolidation Act) the names of defaulters with liabilities (including interest and penalties) in excess of €30,000. Names are published in Iris Oifigiúil. Section 143 of the Finance Act 2005 increased the publication limit from €12,700 to €30,000 where all the tax included in the settlement is tax, the liability in respect of which arose on or after 1 January 2005. Taxpayers who furnish a qualifying voluntary disclosure to the satisfaction of the Revenue Commissioners before any investigation or inquiry had been commenced by them into any matter occasioning liability will not be published. An investigation or inquiry is deemed to have commenced once an examination of the books and records has started. Where, however, there is strong evidence of tax evasion, Revenue may commence an investigation or enquiry before contact has been made with the taxpayer.

Revenue informed the Team that the physical audit files of a Regional Office are stored with the main customer file. Once the electronic audit file is completed, it is 'frozen' in read only mode and removed from the auditor's work list. The Team noted the absence of any defined retention periods for physical or electronic audit files.

Lo-Call Service

A further function of Revenue's Planning Division is to manage at a National level the Lo-Call 1890 service. This service comprises a Virtual Call Centre operating from 17 locations in the country. Each of the four Regions has its own Lo-Call 1890 service Number. All numbers have essentially the same standard message (with minor Regional variations). Revenue stated that all Lo-Call customers are advised that for quality assurance and training purposes, the call is being recorded. Upon further consideration, the Office of the Data Protection Commissioner advises Revenue that 'quality and training' might not cover another key purpose – dispute resolution and complaint handling. Also, the Team were of the opinion that training could perhaps be considered to be implicit in quality requirements. The term 'quality and customer satisfaction purposes' might better capture the purposes of recording such data but this Office considers that this matter is for Revenue to decide upon ultimately. Since the inspection took place, Revenue has indicated its intention to introduce this wording, implementing the change when the messages are next being amended.

The Team notes that the Protocols document states "No calls to an officer, which originate outside of the 1890 system, will be recorded."

Local service managers are required to monitor a percentage of calls for quality and training purposes. Revenue stated to the Team that as all callers' PPSNs are requested in order to handle queries over the phone, call recordings are filed under this reference. Calls to the service have been recorded since 2006 and are used in cases of dispute. It was stated that protocols for the introduction of the recording function were agreed with staff unions. The Team queried as to what format these call recordings were stored and Revenue responded by stating recordings are stored by ICT&L in G729 WAV file format and are code-encrypted. Revenue stated that call recordings are retained for a 4-year period. The basis offered by Revenue for retaining the calls for this length of time is that records are retained for the duration of the time limit for making a claim for repayment of tax. Revenue underlined to the Team that the calls were being recorded only for the purposes stated above and not for any future data mining exercise.

Revenue informed the Team that it also operates a Drugs Confidential Freefone. Credibility checks are carried out where possible against the information being provided. If the information given by the caller is specific enough to facilitate follow-up action or investigation then the details are referred to the appropriate local Unit. Whether or not further action is taken on foot of a call, all Freefone information is logged and retained. Revenue indicated to the Team that the same caller can often call again with updated information, and indeed the same topic can be reported by different callers. Retention of all the original calls is, therefore, considered necessary by Revenue. The Office of the Data Protection Commissioner considers an indefinite retention period to be excessive and advises that a retention period for such data should be devised, taking into account any special considerations regarding the need to co-relate calls over a substantial period of time.

4.2.3 Corporate Services Division (CSD)

The central responsibility to ensure compliance with the Data Protection Acts across Revenue rests with the Data Protection Unit within Corporate Services Division (CSD). Revenue stated to the Team that considerable resources are expended on data protection and that there is strong interest and support in promoting awareness of data protection responsibilities at Board level.

Revenue informed the Team that all new Revenue staff receive data protection training at induction and that data protection is also referenced in certain other training programmes such as Customer Service, Audit and Customs Enforcement training programmes. Directions are provided instructing staff that they must access data only for business purposes. The Team were informed that Revenue's current data protection policy is available on the staff intranet, an updated Security and Confidentiality Policy was re-issued to all staff in January 2009 and a presentation on Information Security ('Protecting the Data that Revenue Holds') was made at Revenue's Senior Management Conference in November 2008. Also, a Revenue Operational Instruction referred to as 'Updated Data Exchange Policy' was issued in July 2008. A further Revenue Operational Instruction was issued in August 2008 entitled 'Data Security Policy Laptops and Electronic Storage Devices used outside of the Office'. This Policy covers security of information/data exchanges arising in the course of compliance work by Revenue's auditors and other outdoor officers. Since the series of inspections took place, Revenue has also forwarded to the Team details of a special Internal Guidance Notice ('Gateway') issued to all Revenue staff in May 2009 which provided specific guidance on eleven key aspects of Data Security.

In addition, the Data Protection Unit within CSD regularly provides advice to colleagues in other parts of the organisation to ensure that particular practices, proposals and developments are compliant with Data Protection legislation.

Revenue acknowledged to the Team that further ongoing training and awareness raising initiatives are needed, indicating its intention to introduce enhanced awareness raising at management level (data protection material will be included in a new foundation management course being developed) and also at operational level alongside enhanced training for existing staff and enhanced induction training. The Team suggested that some additional form of refresher training, communication or other method of raising data protection awareness could be added to the current set of resources, possibly some web accessible tools and information.

Internal Data Protection Checks

Corporate Services Division (CSD) acknowledged that ideally it should have been in a position to undertake an internal data protection audit itself in advance of the ODPC audit. The Team stated that in other similar organisations to Revenue there is a role for Internal Audit functions in determining the effectiveness of data protection policy across the organisation. The Office of the Data Protection Commissioner issued audit guidance for organisations across all sectors in January 2009 and expressed the following view on internal audits

> "Audits referred to as 'self-checks' are frequently conducted in-house by internal control units within organisations themselves or with the assistance of

> external expertise. A data protection audit operates as a control mechanism regardless of whether an organisation self-assesses or is appraised by an independent third party or regulatory body. Checks and appraisals are conducted in order to detect any irregularities or system weaknesses regarding how the organisation handles the personal data of its customers and employees." [4]

The Team were informed that data protection liaison officers within each Revenue Division and Region liaise centrally with Corporate Services Division (CSD). At present, CSD stated they were in the process of dealing with a small number of cases of inappropriate access to Revenue data by staff and is in ongoing liaison with the ODPC on these matters.

Data Transfers

Corporate Services Division (CSD) provided the Team with a document outlining some 21 inbound data transfers from external sources identified by Revenue as taking place across the organisation and underpinned by legislation. The ODPC was also provided with a document outlining statutory provisions that allow for disclosure by Revenue of taxpayer information relating to individuals or companies to third parties.

Notwithstanding the existence of legal provision for the transfer of data, the Team queried the controls over such transfers with CSD. For example, the Team outlined that solely because a legal provision was in place would not justify the general transfer of data to a third party. CSD in response stated it considered there should be a central area overseeing and reviewing requests for new data transfers which should be signed off and implemented by Planning Division with inputs and advice as required from the Data Protection Unit. Revenue subsequently confirmed to the Team that this central area has now been established within Planning Division. Overall, the ODPC would recommend that Revenue be in a position on an ongoing basis to satisfy itself that the legislative basis for each and every data transfer is proportionate.

A Revenue Operational Instruction referred to as 'Updated Data Exchange Policy' was issued by Revenue in July 2008. This Policy covers all information/data exchanges both internally within Revenue and externally with other organisations. Revenue outlined to the Team that a written 'Revenue Data Exchange Agreement' is a mandatory requirement before any data is exchanged with 3rd parties. This Policy covers all information/data exchanges both internally within Revenue and externally with other organisations.

Revenue informed the Team that the majority of transfers of data to 3rd parties are made by ConnectDirect, using a secure Revenue channel. If Connect Direct is not used Revenue stipulate that some form of an appropriate secure online channel must be used where electronic data transfers are involved. Revenue stated that all data transfers by post of memory sticks or CDs ceased at the end of 2008. Revenue outlined to the Team that should any physical transfers of data be necessary the data is encrypted (encryption of USB memory sticks and CDs has been implemented in Revenue) and hand delivered direct by Revenue staff rather than by any third party. In

[4] http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf

relation to transfers to/from third parties such as banks and other agencies, these transfers are required to use either ConnectDirect or GPG encryption. ConnectDirect is monitored by the ICT Operations area in Revenue's primary Data Centre in Dublin. The Team recommends that non-use of Connect Direct should also be monitored and each data transfer outside ConnectDirect logged and reviewed centrally.

Revenue also receives third party data transfers, for example, information on rents from the Department of Social and Family Affairs. An inventory of these transfers was compiled by Revenue in 2008 and updated in 2009 and a copy supplied to the ODPC. The Team observed that the majority of these transfers would appear to be handled through ConnectDirect.

Data Retention

In relation to data retention, Revenue stated that a number of disposals of categories of older records and transfers to the National Archives have taken place. Revenue indicated they have their own requirements to retain records for evidential purposes and have also been advised by the National Archives that where a manual file is to be destroyed, the electronic version should be retained. The Team notes that archiving requirements cited in the Statutory Provisions outlined do not appear to have been addressed in any Revenue policies:

> "National Archives: Under Section 8 of the National Archives Act 1986 Revenue records, including taxpayer records over 30 years old, can be transferred to the National Archives for their retention. However, files relating to taxpayers are certified as not for public viewing by the Revenue Certifying Officer."

From the ODPC perspective, data retention within Revenue and how it is influenced by the requirements of the National Archives Acts and the Data Protection Acts is an area that Revenue must address going forward. Revenue acknowledged to the Team that the retention and disposal of records is an area that will have to be further examined and developed. The Office of the Data Protection Commissioner accepts that this is a complex undertaking and is aware that tension may arise between requirements under the Data Protections Acts not to retain personal data any longer than is necessary and requirements arising where an organisation is subject to the National Archives Act. However, it is the experience of the Office that these tensions can be resolved, once records management and retention of personal data are examined simultaneously and schedules and policies devised with both sets of obligations taken into account.

Project Management

Revenue outlined to the Team that it has a formal and documented process for managing projects, from their origination to implementation and review and that there is a strong governance structure comprising a MAC subgroup (the IT Executive), a Programme Management Office and individual Project Boards. The Team, drawing upon best practice in the public and private sectors, advised Revenue that a privacy impact statement should form part of the assessment process and that there should be formal procedures in place to ensure each project is privacy-proofed. Revenue explained that each Project Board may include CSD membership or draw on CSD views as needed throughout the Project Initiation and Confirmation stages, where

detailed impact analysis is done. Revenue accepted that while privacy aspects are implicitly included in this analysis, the process could be strengthened by the inclusion of a privacy impact statement.

4.2.4 Integrated Business Intelligence System (IBI)

The Integrated Business Intelligence System (IBI) is a portal interface which provides Revenue staff with a comprehensive view of the customer by pulling together data from across Revenue's vast data warehouse. The Team were informed that information on IBI cannot be edited – its function is to give the user an up to date and overall picture of the customer across all interfaces between the customer and Revenue. The information in the data warehouse is updated by Revenue's core systems by way of nightly, weekly, monthly and annual updates.

Access to IBI is managed by the Regions and all access must be approved by the Regional Manager. There are 2,339 users who have access to a number of IBI applications. Revenue stated that this figure represents about 30% of the overall Revenue staff compliment. Within this bracket, there are 'Investigation' type applications that are managed by the Investigations and Prosecutions Division (see 4.2.1 above). Here, access is further restricted, with only 366 users authorised to access Investigation type applications. The largest of these Investigation-type applications is 'Suspicious Transaction Reports' where there are 363 users and the smallest is 'Nursing Home Repayment' investigations where there are 3 users.

Suspicious Transaction Reports (STRs) are money laundering disclosures required to be made to An Garda Síochána by certain financial institutions and other designated persons under Section 57 of the Criminal Justice Act 1994. The Central Bank and Financial Services Authority of Ireland Act 2003 (Schedule 1, Part 17, Item 2) subsequently amended the criminal justice legislation and required reporting entities to submit reports of suspected instances of tax evasion to Revenue, in addition to the existing reporting requirement to An Garda Síochána, with effect from May 2003.

Revenue stated to the Team they have retained all such reports since they first became available in 2003. Under Section 57 of the 1994 Act, as amended, a designated person is required to report to An Garda Síochána and the Revenue Commissioners any instances where there is a suspicion on the part of a designated person that an individual may have been involved in a money laundering transaction. The Team queried how many STRs were filed in 2008 and Revenue stated there were 14,656 STRs received by Revenue in 2008 and approximately 70% of these were received by secure electronic means. The balance was received in hard copy directly into the Suspicious Transactions Reports Office, a unit within IPD.

Citing the following reasons for the permanent retention of all STRs, Revenue explained:

> Firstly, all such intelligence is rated. A significant amount is not deemed appropriate for immediate action or intervention. This is retained. However, other information or intelligence (from STRs or other sources) may come into our possession some time later, perhaps even years later, which we can at that stage relate to the earlier material; thus creating a more significant intelligence package on which we may then decide to act. If the earlier material was not retained, this investigative opportunity would be lost.

> Secondly, several of the STRs received refer back to previous STRs. In other words, there may be numerous STRs about the same taxpayer or company; sometimes from the same reporting entity, sometimes from different reporting entities. (Up to the end of 2007, there were 671 such update reports from different reporting entities and 1,219 such update reports from the same reporting entities, all referring back to previous submissions). If we don't retain earlier reports we cannot reference the new disclosure against the previous material. The second or subsequent STR may have fairly brief information in the knowledge that there was a prior report with fuller details. It would be untenable for Revenue to revert to the reporting entity for details of an earlier report, in such circumstances.
>
> Thirdly, while we may not act on a STR immediately at the time of receipt, it may become relevant some time later, for example when conducting an audit. The STR may have revealed the existence of a relationship with a financial institution or the existence of a certain transaction or transactions, which were not disclosed in the audit. This may result in the institution of an investigation leading to the recovery of additional revenue or to prosecution. In respect of enforcement interventions such as drug trafficking detections, cases have arisen where the STR, though not considered of particular significance at the time of receipt, was critical to the development of the case, when reviewed post detection. It revealed investigative links which could then be pursued. This line of enquiry would have been lost had the STR data not been retained.

Revenue reiterated to the Team that general staff have limited access to IBI. They would not, for example, be able to view VRT data or Suspicious Transactions data.

The Team were informed that all ‘read only’ access on the Integrated Business Intelligence System (IBI) is logged and IT retains a ‘curiosity list’ which notes the access of high profile or sensitive cases. While viewing the system, the Inspection Team noted that a message is displayed at the top of the user’s screen saying that usage is logged and subject to monitoring. If a screen is printed within the IBI systems, the username is displayed on the printout. This functionality is available throughout IBI. The Team considers this practice is to be commended. Revenue clarified that similar functionality was not available in VRT screens as the VRT screens belong to a legacy mainframe system which is scheduled for re-development later in 2009 and into 2010 which will integrate VRT into Revenue’s Integrated Taxation Services (ITS). Revenue subsequently confirmed to the Team that this 'watermark' functionality has now been included in the VRT screens and is available live since end-June 2009.

4.2.5 PAYE System

Revenue’s PAYE system, which is a part of Integrated Taxation Services (ITS), contains some 2.2 million records. There are four Revenue Regions dealing with PAYE customers. Each Region covers a specific geographic area and is further broken down into Revenue Districts (General Claims District - GCD). Revenue informed the Team that the tax affairs of individual staff members in a particular Revenue District are not handled in the office in which the staff member is located but by a Revenue official at another location.

The Inspection Team visited a PAYE processing area in Galway. All physical correspondence received is scanned onto the Integrated Contacts System (iC). The scanned correspondence is assigned by a supervisor to team members by means of a drop down menu. The Team was informed that any amendments made to a customer

record are updated with the amending officer's user id. Scanned documents are held in a filing area within the GCD in date order. Any unscanned documents left over at the end of the day in the CRIO (Central Revenue Information Office) area are locked away by the manager.

Revenue acknowledged to the Team that it was possible to see all the PAYE records on the system, not just those from the local GCD. Revenue indicated that there are business reasons for this; for example, a married couple may be dealt with by different GCDs. Revenue clarified to the Team although it is possible for the supervisor to view correspondence appropriate to another GCD, it is not possible for a supervisor to assign correspondence appropriate to another GCD to a member of his/her team. Subsequent to the audit Revenue has indicated that an individual PAYE staff member can take ownership of and process an item of scanned correspondence. It was stated that this facility is available to help in the operation of Revenue's PAYE lo-call phone service, which deals with calls from PAYE customers. Each Revenue Region has its own lo-call number. There is a security check facility known as 'Audit Trail' built into Integrated Taxation Services (ITS) whereby it was stated that random checks are undertaken by supervisors of processing carried out by their staff for their own GCD and also for other GCDs. This is an issue which will be taken up by ODPC with Revenue as a follow-up to the audit.

Revenue explained to the Team that PAYE customers with other income can also be liable for tax under Self Assessment. Under this system all filing and processing of Returns of Income is dealt with in the Self Assessing area but Tax Credit Certificates are processed in the PAYE area.

Medical Claims

Each GCD deals with claims for medical expenses, which are filed online or in paper format. Revenue stated to the Team that the processing of these claims is non-judgemental. When processed, Integrated Taxation Services (ITS) refunds a number of the claims automatically and sends the balance in the form of workflow to the GCD for approval. A supervisor checks each claim in the workflow for authenticity and accuracy before approval.

Each Region randomly selects cases for further scrutiny. In these cases the customer will be contacted and asked to produce receipts to back up the claim. Revenue stated they do not seek receipts or medical notes, except where a claim is selected for checking, but in some cases a claimant might supply receipts or other unsought documentation. Revenue clarified for the Team that all unsought documentation is returned to the taxpayer at the time the claim is being scanned onto the Integrated Contacts (iC) System for processing - unnecessary receipts and documentation are not scanned.

The Team observed that in the notes accompanying Form Med 1 Health Expenses-Claim for Relief [5] applicants are advised

[5] http://www.revenue.ie/en/tax/it/forms/med1.pdf

> "If your claim is selected for an examination programme and you do not want your own Revenue Office to know the nature of the medical condition, you can ask your Inspector to have the claim examined by another Revenue Office"

This practice is to be commended.

Security

While in the PAYE area, the Inspection Team queried the accessibility of USB ports on staff PCs. A test was undertaken whereby a memory stick was inserted into a PC. While the PC registered the fact that a port had been accessed, it was not possible to access any data on the memory stick.

The Team also inspected the email inbox/outbox of a staff member. The Team indicated to Revenue that this type of spot check was sometimes undertaken in the course of a data protection audit in order to ascertain if procedures around privacy and confidentiality are being adhered to at a local level. The Inspection Team viewed a number of emails and attachments and was satisfied that there was no inappropriate transfer of personal data discernible or evidence of any security protocols being compromised.

Payment of Capital Gains Tax

The Team queried the notes on the back of Revenue forms such as CGT Payslip B[6] regarding the method of payment which stated "Always write your PPS Number on the back of your cheque". Since the inspection took place, Revenue have issued clarification regarding this practice, stating

> "While the practice is a longstanding one, there is still a valid rationale in asking for a PPSN in that many taxpayers make payments without giving any accompanying correspondence or documentation that would enable Revenue to appropriate the payment. Even today, we still receive cheques in the post with no other documentation. There isn't necessarily a correlation between the bank account name and the tax registration that is to be credited with the payment. At least with a PPSN on the back of a cheque, we have some means of correctly identifying the relevant tax registration.
>
> In relation to Capital Gains Tax, this is an event tax and a taxpayer may find themselves liable to pay the tax, without being registered for it. In order to appropriate the payment, the taxpayer has to be registered first. With a PPS number we can register someone for the tax and appropriate the payment. Also, when we ask customers to include their PPSNs on the back of cheques the customers are aware that the cheque will eventually make its way back to the bank."
>
> In summary, it is considered that the request for the taxpayer's PPSN is still a valid request in order to appropriate payments and it also serves to minimise delays in processing the taxpayer's payments and updating their tax record.

Revenue also supplied the Team with extracts from internal instructions: Tax memo 34/2002 and a page from Revenue's Local Payment Accounting (LPA) User Guide. Tax Memo 34/2002 etc. states that in the event that a cheque is returned unpaid, the 'customer number' etc. will enable the payment to be traced and cancelled from the customer's account.

---

[6] http://www.revenue.ie/en/tax/cgt/forms/cgtb.pdf

The Office of the Data Protection Commissioner concludes that the 'customer number' is in practice deemed to be the PPSN and notes that Revenue's entry in the PPSN register of Users on the Department of Social & Family Affair's website states that the PPSN " is used as an individual's Tax Reference number"[7].

While ODPC accepts that there is a valid operational reason for seeking the writing of a PPSN on the back of cheques, it undoubtedly increases the risk of fraud or identity theft for such individuals as their cheques are processed in the banking system. It is a key piece of additional personal data that will be available to any person within the banking system (in addition to bank account, sort code, signature, etc) minded to use the information for illegal purposes. The issue of lack of identification of cheques can be dealt with by the provision of more information to taxpayers when sending cheques and it is recommended that the practice of seeking the PPSN in this manner on the back of cheques be revisited.

4.2.6 Information & Communications Technology and Logistics Division (ICT&L)

ICT&L carries out Revenue's IT functions. ICT&L's primary Revenue Data Centre is situated in Dublin with a mirror Data Centre in another Dublin location. Revenue stated that it is envisaged that the main Dublin site will continue as Revenue's IT centre for the next 3-5 years at least.

Revenue outlined to the Team that they augment their internal teams by external resources from a variety of vendors. Revenue confirmed to the Team that contracts with all external resources or consultants address security and confidentiality, including a data protection clause. External resources are also obliged to sign the Official Secrets Act. Unless assigned to a Live Support team, Revenue stated that external resources have access to test data only.

Access to systems

In order to access any Revenue system, an initial access level is required for the core system followed by further logon controls to the individual business systems. The Team were informed that access to all applications is either by token (swipe card) plus password, or by user id plus password.

Revenue stated to the Team that access levels to Revenue systems also depend on where a Revenue employee works. If a staff member leaves a particular area, their access rights are removed and reset if moving to a new area. The Inspection Team was provided with a copy of the documented procedures in use at Revenue's IT Service Desk. Requests for new user accounts must be completed by a local IT liaison officer or a local administration section and sent through the IT Service Desk Requests System. This process sets up the user's account and email, but the Team were informed that actual access to individual business systems must be granted at a local or regional level. Access to the business systems cannot take place unless the basic user account has been generated. If a user account has been unused for a period of time, it is locked. The Team were informed that unused user accounts are

[7] http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx#rev

automatically 'expired' by the system after 45 days and that such accounts must then be re-enabled by the IT Service Desk. After 240 days of continued non-use, such accounts are automatically disabled by the system (removal of access rights etc).

Revenue outlined to the Team that tax practitioners can register with Revenue in order to conduct their business over a secure email link. Some 2,000 agents, accountancy firms and business taxpayers have signed up to conduct their business in this way (this would include some 3,000 individuals within these firms). Replies being issued to incoming secure emails from practitioners are automatically encrypted. Revenue stated to the Team that the total number of Revenue customers who operate as agents, accountancy firms and business taxpayers is far in excess of the number who are currently signed up for secure email. From a data security perspective, the Office of the Data Protection Commissioner stated it would endorse any Revenue efforts designed to encourage more entities in this sector to sign up to avail of secure mail services.

Audit Trails

All of the main Revenue business systems including IBI, and ITS (Integrated Taxation Services which covers all taxes and duties including PAYE) have both read and write audit trail logging.

In order for a matter of inappropriate access or usage to come to the attention of Revenue, Revenue stated that some suspicion at local level would be required. The matter would then need to be reported by a local manager upwards to ICT&L and to the Data Protection Unit in Corporate Services Division. The Team outlined to Revenue that procedures should be devised and implemented by Revenue whereby staff members' access to systems would be reviewed periodically on a random basis by local and regional managers. The Team cited An Garda Síochána (AGS) as having successfully adopted such a policy in relation to access by AGS members to PULSE.

Batch transfers of personal data

The Team were informed that Revenue's batch data transfers are conducted using ConnectDirect. ICT&L has enhanced the product by adding Secure+ which provides configurable authentication and encryption. ConnectDirect allows for high-volume point-to-point file transfer and guarantees delivery of files within and between organisations. Revenue stated to the Team that ConnectDirect is recommended by the Irish Banking sector and has been in use in Revenue since 2001. Revenue has 21 ConnectDirect transactions of which 16 are with financial institutions involving, for example, the transfer of mortgage relief details in order to update Revenue's TRS (Tax Relief at Source) system. The remaining 5 data transfers involve other government departments and agencies and health insurance companies.

Revenue stated that all transfers with financial institutions are bound by a Data Exchange Agreement which was provided to the Team. This agreement sets out the type of data required to be transferred, specific contact persons and frequency of the exchanges. Financial institutions transferring data to Revenue each have their own unique identifier within the TRS system. Inbound file transfers hold this identifier and file date as part of the inbound file name. This ensures that the system can recognise and allocate data transfers within the TRS system correctly. Any updates from a data

transfer are automatically made available to users within the TRS system, thus removing the need to issue any results by email or printout.

The Inspection Team was provided with a step-through of how a batch transfer takes place, using the example of an outbound transfer of PRSI information to the Department of Social and Family Affairs.

Revenue indicated that all of the organisation's legacy systems in this area have, at this point, been replaced and this has eliminated all smaller data transfers or ad-hoc transfer arrangements which may previously have taken place. All internal and external data transfers are bound by Revenue's Data Exchange Policy which required upon issue the automated acknowledgement of all Revenue staff.

The Team were informed that a historic directory retains a copy of the file which has been sent through the ConnectDirect transfer process. These files are backed up and purged at regular intervals.

Laptops

Revenue stated there are some 1,200 laptops in use throughout the organisation. A laptop is assigned to a named individual on foot of a request from his/her local manager. A register of all laptops is held within Revenue's 'Financials' database.

Revenue informed the Team that laptops are encrypted as standard practice. Revenue stated its testing of the strength of laptop encryption and security was done formally with the assistance of an international security company.

Business laptops offer remote access to systems. Information being received by an outdoor officer from an organisation is transferred directly into Revenue's systems or brought immediately to the office, transferred and deleted from the laptop. This is outlined in detail in Revenue's Laptop Security Policy. Mass storage devices are also encrypted. Even with such policies in place, Revenue acknowledged that there is no absolute way of confirming that an officer does not have personal data held on a laptop. The Team considers that if business laptops offer remote access to systems, Revenue should examine the possibility of disabling access to applications facilitating the storage or import of personal data onto laptop hard drives.

Revenue stated it must rely on the word of an officer in a case where a laptop has been lost or stolen. Revenue stated it had recently put data protection breach notification procedures in place. Loss or theft of a laptop is reported to the IT Service Desk, the designated Security Officer in ICT&L Division and the Data Controller in Corporate Services Division. Revenue indicated that it has a formal security officer role for the maintenance of corporate IT security standards. The Team referred Revenue to guidance regarding breach notification on the ODPC website[8].

[8] http://www.dataprotection.ie/docs/Breach_Notification_Guidance/901.htm

Biometrics
Revenue informed the Team it had examined the possibility of introducing biometric identification, as a method of sign-on authentication to some of its information systems, but decided, on balance, not to pursue this particular course.

General Security & CCTV
The Team were informed that the primary IT Centre in Dublin has a 24 hour security presence (an outsourced commercial security company) and that all staff enter and leave areas within the building using swipe cards. Revenue confirmed to the Team that CCTV is in use both inside and outside the site, though the Team commented that no signage was erected to signify that cameras were in use externally. Revenue informed the Team that An Garda Síochána had recently undertaken a security audit of the facility and found that the lack of identifying signage at the entrance gate to the facility was of benefit from a security aspect in that the facility wasn't 'advertising' or drawing attention to itself.

The Office of the Data Protection Commissioner accepts there are high security requirements in relation to the primary IT Centre site in order to maintain the 'low key' aspect of the facility. The Team noted a sign saying 'CCTV in use' behind the main desk in the Reception Area inside the door to the building. The Team advised that the security purpose is taken as implicit in the wording but the signage would need to be changed should there be any other purposes for which the CCTV was being deployed.

5. FINDINGS

Excellent co-operation was received throughout the inspection. The Inspection Team considered that there exists a very high organisational awareness of data protection principles in Revenue. In particular, the presence of a dedicated Data Protection Unit, with designated contact points in the event of any issues arising was considered by the Team to be a very appropriate structure for a public sector entity in possession of high volumes of personal data.

There is very clear evidence that a detailed approach has been taken by Revenue to identifying and setting out, via policy documents etc, its responsibilities under data protection legislation. This thorough approach is to be welcomed. However, it is also evident that there are areas for further improvement in relation to aspects of data protection compliance monitoring to ensure that this commitment is reflected in actual practice and standards on the ground. The ODPC would expect that Revenue will be seeking to improve its focus in this area on foot of this audit.

The issue of data retention was a recurring theme throughout the course of the audit. The Team noted throughout the inspection the absence of a retention policy or schedules at either micro or macro-level within the Revenue Commissioners. An overriding impression was formed of an organisation where paper documents and electronic files are retained indefinitely on a 'just-in-case' basis.

Section 2(1)(c) of the Data Protection Acts 1998 and 2003 provides that a data controller shall not retain personal data longer than is necessary for the purpose or purposes it was obtained. Accordingly, the ODPC recommends that Revenue deletes any such personal data that is no longer required for legitimate business purposes and implements a defined policy on retention periods for all items of personal data kept by the organisation (both manually and electronically). The recommendations in section 6 below single out areas examined during the inspection for priority.

The practice whereby claimants for tax relief for medical expenses are offered the opportunity to have such claims, which contain health data (sensitive personal data in terms of the Data Protection Acts), examined by another Revenue office is to be commended.

As this report makes clear, Revenue and its staff have access to a very large amount of personal data in relation to almost everyone in the State. The power of Revenue to demand such data using statutory powers has increased significantly in recent years. The capacity to generate a "single view" of the taxpayer through mining of internal ICT systems gives access to a very detailed profile of the individual - not only their income and tax details, but information about their family relationships, housing, education, transport and medical conditions. Some of these are formally "sensitive data" under data protection legislation. But public opinion surveys show that financial data, though not formally "sensitive data", is considered by Irish people as the type of data that they most want to be kept private.

This situation imposes a heavy obligation on Revenue to ensure that the personal data it holds is kept securely and that access to it is strictly limited on a "need to know" basis. It also should lead to Revenue carrying out a formal Privacy Impact Assessment of any proposals to extend its investigative remit that involve the capture of additional items of personal data. This is particularly important in the case of proposals to give Revenue access to external databases. As a baseline for such activity, Revenue should carry out a comprehensive review of the proportionality of existing access to such external data sources.

6. RECOMMENDATIONS

Proportionality of Personal Data used

- Revenue should satisfy itself that the legislative basis for each and every data transfer is proportionate.
- Revenue should carry out a comprehensive review of the proportionality of existing access to external data sources.

Revenue Response: Revenue accepts these recommendations.

- Revenue should carry out a formal Privacy Impact Assessment in relation to any proposals to extend its investigative remit involving the capture of additional items of personal data.

Revenue Response: Revenue will examine this recommendation.

Retention:

- A retention policy needs to be devised to ensure that files no longer required in the Criminal Investigations Area are archived or disposed of securely and safely, taking into account any special considerations regarding the need to retain records for use as evidence in prosecutions etc.

Revenue Response: Revenue accepts this recommendation.

- A retention period for call recordings to the Drugs Confidential Freefone No. should be devised, taking into account any special considerations regarding the need to co-relate calls over a substantial period of time.

Revenue Response: Revenue accepts this recommendation.

- A retention policy should be devised to ensure that physical or electronic audit files are archived or disposed of securely and safely. The ODPC would consider that it is not appropriate to retain all STRs received on an indefinite basis. This is especially the case as the number of such reports is likely to increase considerably once the Third Anti-Money Laundering Directive is transposed domestically.

Revenue Response: While Revenue considers that the specific reasons provided for the retention of STR reports (as set out in detail in Section 4.2.4) are still valid, we also confirm that the ODPC's views will be further considered in the context of the development of a data retention policy.

.

Data Transfers

- It is recommended that non-use of Connect Direct should also be monitored and each data transfer outside ConnectDirect logged and reviewed centrally.

Revenue Response: Revenue accepts this recommendation.

Laptop Security

- Revenue should examine the possibility of disabling access to applications facilitating the storage or import of personal data onto laptop hard drives.

Revenue Response: Revenue accepts this recommendation.

Data Protection Compliance Monitoring

While the focus on data protection matters in Revenue is not in doubt and the role of the Data Protection Unit in this respect is clear, there remain areas for further improvement in relation to aspects of internal monitoring within the organisation. Most notable in this respect is that there is a need for further ongoing internal monitoring of compliance with data protection requirements. This should be

addressed and this role should be undertaken either by the Data Protection Unit or by the Internal Audit Unit as part of its functions.

- An effective means of reviewing internal compliance with data protection requirements should be introduced.

Revenue Response: It is intended that the Internal Audit Plan for 2010 will include an audit of the security of personal data. The audit will be a joint audit led by Revenue's Internal Audit Branch and with the Data Protection Unit actively participating in and supporting the Audit.

Equally the examination of access to taxpayer information only in response to complaints received from members of the public or this Office is not considered to represent a sufficiently significant deterrent to inappropriate access to such information given the very limited number of such complaints. Such incidents when reported are, of course, treated with the upmost seriousness by Revenue.

- Further procedures should be devised and implemented by Revenue whereby staff access to systems containing personal data is further reviewed periodically on a random basis by local and regional managers.

Revenue Response: Revenue accepts this recommendation.

- Future deployments of Business Analytics tools examining 'peak and trough' usage data regarding activity on an individual record over a specified period of time, could be expanded to incorporate read only access or 'look-ups' as well as the current practice to examine 'edits' to individual records.

Revenue Response: Revenue is currently looking at the further development of its Business Analytics tools to assist with internal monitoring.

PPSN

- The policy of seeking the writing of PPSNs on the back of cheques should be further considered in light of the points made in the report.

Revenue Response: This particular policy will be further considered in the light of the points made in this report.