Protection of Personal Data

in the

Valuation Office

Code of Practice

24 May 2018

Table of Contents

Introduction

1.1 The Valuation Office is the State property valuation agency. The core business of the Office is the maintenance of equitable Valuation Lists through the provision of accurate, up-to-date valuations of commercial and industrial properties to ratepayers and rating authorities as laid down by statute. The Office also provides, where possible, a non-statutory valuation consultancy service to other Government departments and State Agencies.

1.2 All data, including information and knowledge, is essential to the administrative business of Departments and Offices of State. In collecting personal data, the Valuation Office has a responsibility to use it both effectively and ethically. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of the Office.

1.3 Therefore, it is critical that public servants work to the highest attainable standards. Our integrity includes both the way in which we conduct ourselves and the way in which we ensure the data we hold is compliant with relevant legislation.

1.4 Up until recently the Data Protection Acts 1988 and 2003 were the main legislation to consider in relation to protection of personal data. However, an EU regulation and an EU directive are coming into effect on 25th May 2018. The regulation is the General Data Protection Regulation, provided for in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. The directive is Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

1.5 The Data Protection Bill 2018 is going through the legislative process and intends to give effect in Irish law to the law enforcement directive. The aim of this Code of Practice is to ensure that each employee of the Valuation Office has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This in turn, will assist the Office in its compliance with the Acts, regulation and directive.

1.6 Protection of our data is common sense as we need to ensure that data gathered and processed by the Office is compliant with Data Protection Legislation. The reading and understanding of this code by all employees will go a long way towards meeting this requirement. Further advice in relation to the storage, handling and protection of personal data is available in the Department of Finance "Guidance Note, dated December 2008, on protecting the confidentiality of Personal Data.

Commissioner of Valuation

Glossary

2.1 Appendix 1 contains a Glossary of the key terms used in this Code of Practice.

Data Protection Rules

Types of Personal Data held by the Valuation Office

3.1 The Valuation Office is registered as a Data Controller with the Office of the Data Protection Commissioner (Registration number 0422/A). Particulars of our registration are available on-line at www.dataprotection.ie.

3.2 The Valuation Office would typically retain and process the following types of personal information which is included in the Human Resource Management System (HRMS) and in the salary payment system (Corepay):

* Employee's Name, Address, Gender, Date of Birth, name of next of kin.

* Name of Employee's next of kin, address of next of kin.

* Employee's Personal Public Service Number (PPSN), income detail, bank account holder's number and/or other financial details. Income tax detail; pension purchase detail; trade union membership detail.

* Employee's sick leave detail and/or other disability detail.

* Employees service detail such as length of service and other related data held in the personal record file.

3.3 The Valuation Office would typically retain and process the following types of customer/ratepayer's personal information which is included in the revision VO Worklist System, in the revaluation Workflow System, hardcopy and digital property files, hardcopy and digital 1st appeal files, hardcopy & digital valuation tribunal files & hardcopy and digital market value files & applications for information to the public office.

Occupier's/Ratepayer's home address details

Occupier'/ratepayer's private contact phone & e-mail details

Market Information details in relation to occupier's/ratepayer's property

Financial information in relation to occupier's/ratepayer's property

Obligations of the Valuation Office

4.1 The Valuation Office controls the contents and use of certain Personal Data provided to it in the course of its business. Such information typically includes names, addresses, and other contact details such as private phone numbers & e-mail addresses of individual property owners, lessors and occupiers and sometimes, the details of the property market transactions and/or financial information relating to their businesses which are required in the processing of valuation work and the business requirements of the Office.

What the Valuation Office does with Personal Data

5.1 Within the meaning of the Data Protection Acts and GDPR, the Valuation Office processes personal data for payroll production, human resource management purposes and for the provision of valuation services. Payroll & human resource management data is available internally only to the Personnel/Finance Officer and to staff directly under her control, who are employed as appropriate on payroll duties in the Accounts Unit and the Personnel Unit. The Chief Medical Officer for the Civil service is given access to sick leave records from the Human Resource Management System (HRMS). Access to the personal details of an occupier and/or ratepayer is restricted to internal VO staff.

Collection, Processing, Maintaining and Disclosure of Personal Data

6.1 The Valuation Office is obliged to comply with the data protection principles set out in section 2 of the Data Protection Acts 1988 and 2003 and Article 5 of the GDPR. These obligations mean that the personal data held by the Office must meet the following criteria.

6.2 Must be obtained and processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'.

As all personal data has been provided to the Valuation Office by employees, by transferring Departments, Offices and Agencies, by the Public Appointments Service, by ratepayers or local authorities the Office will regard such data as having been fairly obtained. Reference to this code and how to request/view a copy is provided to employees. Application forms set out the data protection rights of data subjects.

6.3 Shall be accurate, complete and kept up to date

By completing and signing a form tendering personal data to the Valuation Office, its employees are indicating that the information being provided is accurate and true in every respect and similarly, information received from the Public Appointments Service (central recruiting agency) or from other transferring Departments is accepted as accurate and true. The Valuation Office cannot accept responsibility for inaccurate information provided by any employee either in error or on purpose. Notwithstanding this, the Valuation Office will endeavour to ensure that Personal Data processed by the Office is accurate, complete, and up to date.

The Valuation Office will also comply with any data rectification/ erasure requests received under Section 6? of the Data Protection Acts and Articles 16 and 17 of the GDPR in accordance with paragraph 12 below.

6.4 Shall have been obtained only for one or more specified, explicit, legitimate and lawful purpose.

The Valuation Office processes Personal Data that it holds in respect of its employees only for the purposes for which it was obtained, e.g. recruitment, payroll processing, other necessary accounting procedures and for the administration of the personnel functions of the HRMS.

The Valuation Office processes Personal Data that it holds in respect of its customers (property occupiers and/or ratepayers) only for the legitimate business requirements of the Office for which it was obtained.

6.5 Must not be processed for incompatible purposes

The Valuation Office will not process Personal Data for purposes otherwise than in compliance with and in discharge of its functions.

6.6 Shall be adequate, relevant and not excessive for those purposes

The Valuation Office only requires the level of Personal Data which is relevant to the discharge of its functions. It does not seek, nor does it wish to receive, excessive levels of data which are not relevant to its functions.

6.7 Shall not be kept no longer than is necessary

The Valuation Office subscribes to the policies of the National Archives as enunciated in statute to transfer its records to that body for preservation when they are 30 years old unless they are required for official purposes or if their disposal has been authorised by the Director of the National Archives in accordance with the provisions of the National Archives Act, 1986.. The National Archives is subject to the same data protection requirements as the Valuation Office.

6.8 Must be kept secure against unauthorised access, alteration or destruction

The Valuation Office uses robust IT management systems with restricted access to ensure the security of its data. The Office has established appropriate security provisions to ensure that:

(a) Access to its computer systems is restricted to authorised staff.

(b) Its systems are password protected.

(c) There are comprehensive back-up procedures in operation.

(d) In accordance with our security obligations under the Data Protection Acts, our systems are regularly backed-up so as to avoid the loss or compromise of data. Backed-up data is held specifically for the purpose of recreating a file in the event of the current data being destroyed. Back-up data will not ordinarily be provided in response to a Data Access Request.

(e) Paper files containing personal data are locked away securely when not in use.

6.9 Obligation on staff to access data only on a need to know basis

There is an explicit obligation on staff working in the Valuation Office to access data on a need to know basis only, i.e. for the purposes of performing the work which has been allocated to them.

Right of Access

7.1 Under Section 4 of the Data Protection Acts and Article 15 of the GDPR, Data Subjects are entitled to the following information from the Valuation Office:

(a) Confirmation as to whether the Office keeps Personal Data relating to them.

(b) A description of the categories of Personal Data processed.

(c) A copy of such Personal Data in intelligible form. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy of a data subject's personal data shall not adversely affect the rights and freedoms of others.

(d) A description of the purpose(s) for processing the Personal Data.

(e) The identity of those to whom the Office has disclosed or currently discloses the data.

(f) The source of the Personal Data (unless this is contrary to the public interest).

(g) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(h) the existence of the right to request from the Valuation Office rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(i) the right to lodge a complaint with the Data Protection Commissioner;

7.2 Access requests under Section 4 of the Data Protection Acts and Article 15 of the GDPR apply to Personal Data held by the Valuation Office in its computer systems and in manuscript format within a relevant filing system. However, where a document exists in duplicate, e.g. where correspondence is scanned into our systems, two copies of the same document will not be provided in response to the same request.

7.3 **The Data Protection (access Modification) (Health) Regulations, 1989 (S.I. No.82 of 1989):** The Data Protection (Access Modification) (Health) Regulations, 1989 (S.I. No. 82 of 1989) provide that health data, relating to an individual should not be made available to the individual, in response to a Data Access Request, if it would be likely to cause serious harm to the physical or mental health of the Data Subject.

In the event that these regulations apply, the health data in question will not be provided to the Data Subject but will, however, be furnished to the Data Subject's own authorised medical practitioner.

Formalities for Data Access Requests

8.1 A Data Access Request must meet certain requirements as specified in the Data Protection Acts:

(a) It must be in writing;

(b) It must include a reasonable level of appropriate information to help locate the data required (however, no reason for the request needs to be provided).

(c) The Valuation Office will make reasonable enquiries to satisfy itself about the identity of the person making the request to ensure that disclosure of Personal Data is not being made to a party not entitled to it.

(d) In keeping with Article 12 of the GDPR, the Valuation Office will generally consider a Data Access Request free of charge.

However, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the Valuation Office may either:

(a) Charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) Refuse to act on the request.

8.2 Timeline for the supply of Personal Data

(a) As set out in Article 12 of the GDPR, Data Access Requests will be complied with within one month of receipt of the request. This period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where reasonable additional information is required to substantiate the request as described in paragraphs 7.1 (b) and (c), the timeframe for responding will run from the date of receipt of the additional information.

(b) If the Office receives a very general Data Access Request, e.g. "please give me all the information which you hold on me", the Data Protection Acts allow the Office to seek more detailed information on the nature of the request, such as the approximate date of a particular incident, the Office reference number, the identity of the other party, etc. However, this will be assessed on a case-by case-basis.

Information which will not be provided

9.1 The Valuation Office will not normally disclose the following types of information in response to a Data Access Request:

Information about other people

A data Access Request may cover information which relates to one or more people other than the Data Subject. The information about the other person may be Personal data about that person, to which the usual data protection rules under the Data Protection acts, including the restrictions on disclosure, apply. In such circumstances, the Office will not grant access to the information in question unless either;

(a) the other person has consented to the disclosure of their data to the Data Subject; or

(b) in all the circumstances it is reasonable to make the disclosure without that person's consent.

If the person's consent is not forthcoming and it is not reasonable to make the disclosure without consent, the Office will make available as much Personal Data as possible without revealing the identity of the other person e.g. by excluding the person's name and/or other identifying particulars).

9.2 Opinions given in confidence

Where the Valuation Office holds Personal data about the Data Subject in the form of an opinion given in confidence, we are not required to disclose such opinions in response to a Data Access Request in all cases.

9.3 Repeat Requests

The Data Protection Acts provide for an exemption in respect of repeat requests where an identical or similar request has been complied with in relation to the same Data Subject within a reasonable prior period. The Valuation Office will consider that if a request is made within a period of six months of the original request and where there has been no significant change in the personal data held in relation to the individual, it will be treated as a repeat request. Accordingly, where Personal Data has recently been provided to the Data Subject or his/her legal representative, the Valuation Office will not normally provide a further copy of the same data in response to Data Access Request. The Valuation Office will not consider that it is obliged to provide copies of documents that are in the public domain.

9.4 Privileged Documents

Where a claim of privilege could be granted in court proceedings in relation to communications between an individual and his/her professional legal advisers (or between those advisers) any privileged information which the Office holds need not be disclosed pursuant to a Data Access Request.

9.5 Refusal of a Data Access Request

Where the Valuation Office refuses a Data Access Request, it will do so in writing and will set out the reasons for its refusal to comply with the Request. Any person who is aggrieved with the response of the Valuation Office to their request has the right to make a complaint to the Data Protection Commissioner.

Exceptions to Right of Access to Data

10.1 Section 5 of the Data Protection Acts and Article 23 of the GDPR provides that individuals do not have a right to see information relating to them where any of the following circumstances apply:

(a) If the information is kept for the purpose of national security, or defence, or public security; 4.5.2016 L 119/46 Official Journal of the European Union EN preventing, detecting or investigating offences, apprehending or prosecuting offenders, or in assessing/collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities;

(b) If granting the right of access would be likely to impair the security or the maintenance of good order in a prison or other place of detention;

(c) If the information is kept for certain anti-fraud functions; but only in cases where allowing the right of access would be likely to impede any such functions;

(d) If granting the right of access would be likely to harm the international relations of the State;

(e) If the information concerns an estimate of damages or compensation in respect of a claim against the organisation, where granting the right of access would be likely to harm the interests of the organisation.

(f) If the information would be subject to legal professional privilege in court;

(g) If the information is kept only for the purpose of statistics or carrying out research, but only where the information is not disclosed to anyone else, and where the results of the statistical work or research are not made available in a form that identifies any of the individuals involved.

(h) Other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security;

(i) The protection of judicial independence and judicial proceedings;

(j) The prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

(k) A monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (h) and (i);

(l) The protection of the data subject or the rights and freedoms of others;

(m) The enforcement of civil law claims.

2. In this regard, In particular, any legislative measure referred to in paragraph 10.1 shall contain specific provisions at least, where relevant, as to:

(a) The purposes of the processing or categories of processing;

(b) The categories of personal data;

(c) The scope of the restrictions introduced;

(d) The safeguards to prevent abuse or unlawful access or transfer;

(e) The specification of the controller or categories of controllers;

(f) The storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;

(g) The risks to the rights and freedoms of data subjects; and

(h) The right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

Format of the Response

11.1 The Data Protection Acts provide a right of access to a permanent copy of the Personal Data that is held about the Data Subject unless this is not possible or involve disproportionate effort.

11.2 The information must be communicated to the Data Subject in an intelligible form. Usually, this will mean that a photocopy or print-out of the Personal Data will be provided to the Data Subject. However, where a Data Subject agrees, information can be provided in electronic format, by email or on disk.

Data Portability

12.1 Article 20 of the GDPR provides that a data subject has a right to obtain their data from one organisation and have it transferred to another organisation.

Rectification or Erasure

13.1 If a Data Subject seeks to have any of his/her Personal Data rectified or erased, this will be done within one month of his/her request being made provided there is reasonable evidence in support of the need for rectification or erasure.

Disclosure of Personal Data Outside of the EEA

14.1 The Valuation Office will not ordinarily transfer Personal Data to countries outside the European Economic Area (EEA). In the event that this position changes, the Valuation Office will comply with its obligations under Section 11 of the Data Protection Acts by adopting one of the appropriate measures approved by the Data Protection Commissioner to ensure such transfers are lawful. In addition, the Valuation Office will satisfy the requirements in Chapter V, ***Transfers of personal data to third countries or international organisations of the GDPR.***

Responsibility of Employees

15.1 All employees of the Valuation Office have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this Code of Practice in accordance with the policies and procedures of the Office.

15.2 All employees are charged with the responsibility of ensuring that all data that they access, manage and control as part of their daily duties is carried out in accordance with the Data Protection Acts and this Code of Practice.

15.3 Employees found in breach of the Data Protection rules may be found to be acting in breach of or, in certain circumstances, committing an offence under the Data Protection Act, 1988 and 2003 and/or the GDPR. All current and former employees of the Office may be held accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the Office.

Audits of Procedures

16.1 The Audit Committee of the Valuation Office, when determining in consultation with the Accounting Officer the work programme of the Internal Audit Unit, will ensure that the programme contains adequate coverage within the Office of areas which are responsible for the storage, handling and protection of personal data.

16.2 The particular focus of any audit review will be on assessing the adequacy of the control systems designed, in place and operated in these areas for the purpose of minimising the risk of any breach of the data protection regulations.

16.3 Risks associated with the storage, handling and protection of personal data will be included in the in the Office's risk register and risk assessments will be undertaken as part of the Office's risk strategy exercise. External audits of all aspects of Data Protection within the Office may be conducted on a periodic basis by the Office of the Data Protection Commissioner.

Protocol for Reporting Breaches

17.1 If any breaches of the code of practice or of the regulations occur, the Office's Breach Management Plan (Appendix 3) will be followed.

Appendix 1

Glossary

Data - Information in a form which can be processed. It includes both automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Data Access Request is a request made in writing to a Data Controller of an organisation by a Data Subject for the disclosure of their personal data pursuant to Section 4 of the Data Protection Acts and Article 15 of the GDPR.

Data Controller is a person who, either alone or with others, controls the content and use of personal data.

Data Processing is the performing of any operation or set of operations on data, including:

(a) Obtaining, recording or keeping data,

(b) Collecting, organising, storing, altering or adapting the data,

(c) Retrieving, consulting, or using the data,

(d) Disclosing the information or data by transmitting, disseminating or otherwise making it available,

(e) Aligning, combining, blocking, erasing or destroying the data.

Data Processor is a person who processes personal data on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of his/her employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Acts place responsibilities on such entities in relation to their processing of the data.

Data Protection Acts – the Data Protection Acts 1988 and 2003 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information. This applies to personal information relating both to employees of the Valuation Office and individuals who interact with the Office.

Data Subject is the person who is the subject of the Personal Data. Only a Data Subject is entitled to make a Data Access Request.

General Data Protection Regulation provides for **the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repeals Directive 95/46/EC. It is** contained in **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**

Manual Data is information that is kept as part of a relevant filing system, or with the intention that it should form part of a relevant filing system.

Personal Data – Data relating to a living individual who is or can be identified either from the data or the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. This can be a very wide definition, depending on the circumstances.

Relevant Filing System – Any set of information that is structured or organised by name, PPSN (if applicable in an organisation), payroll number, employee number or date of birth or any other unique identifier would all be considered relevant.

Sensitive Personal Data – relates to specific categories of data which are defined as data relating to a person's racial origin; political opinions or religious or other beliefs, physical or mental health; sexual life; criminal convictions or the alleged commission of an offence; trade union membership.

Appendix 2

Enforcement of Data Protection Legislation

Date Protection Commissioner

The Data Protection Acts established the independent Office of the Data Protection Commissioner. The Commissioner is appointed by Government and is independent in the performance of his/her functions. The Data Protection Commissioner's function is to ensure that those who keep personal data in respect of individuals comply with the provisions of the Data Protection Acts including the GDPR.

The Commissioner maintains a register, available for public inspection, giving general details about the data handling practices of a range of data controllers, such as Government Departments, state agencies and financial institutions.

The Data Protection Commissioner has a wide range of enforcement powers to assist in ensuring that the principles of Data Protection are being observed. These include the serving of legal notices compelling a data controller to provide information needed to assist his enquiries, compelling a data controller to implement a provision in the Act, etc.

The Data Protection Commissioner also investigates complaints made by the general public in relation to personal data and has wide powers in this area. For example, the Commissioners may authorise officers to enter premises and to inspect personal information held on computer or relevant paper system. Members of the public who wish to make formal complaints may do so by writing to the Office of the Data Protection Commissioner, Canal House, Station Road, Portarlington, Co. Laois, or by email to info@dataprotection.ie

Where employees of the organisation, in the normal course of their duties, become aware that an individual including employees of the organisation may be breaching the Acts or have committed or are committing an offence under the Acts, they should report the matter to Ms. Mary Smyth, Personnel Officer, Tel: 817 1004 & email: mary.smyth@valoff.ie

A data controller found guilty of an offence under the Data Protection Acts can be fined up to €100,000 on conviction and/or may be ordered to delete all or part of a database if relevant to the offence.

Article 83 of the GDPR provides for administrative fines up to €20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher

Advice/Assistance

All requests for advice and assistance on data protection issues within the organisation should be directed to Mr. Cillian Byrnes, Data Protection Officer, Tel: 817 1006 and email: cillian.byrnes@valoff.ie

Applying for Access to Personal Data

Requests for personal data should be made in writing to Mr. Cillian Byrnes, Data Protection Officer, Tel: 8171006 and email: cillian.byrnes@valoff.ie

Responding to Requests

When a valid request is received, the Organisation must reply within one month*, even if personal data is not held.

Useful contacts

Data Protection Commissioner's Office,
Phone: 1890 252231,
http://www.datprotection.ie
info@dataprotection.ie

*21 days if the requester is to be informed if any personal data is held and to be given a description of the data and the purpose for which they are kept (Section 3 of the Data Protection Acts).

Appendix 3

Breach Management Policy

This policy sets out the issues that the Valuation Office needs to consider in the event of a security breach involving the loss of the personal data defined at par. 3.2 in the Code of Practice in relation to the Protection of Personal Data in the

Office. It is designed to comply in particular with Article 33 **Notification of a personal data breach to the supervisory authority and Article 34 Communication of a personal data breach to the data subject of the GDPR** It is not intended to be legal advice and is not a comprehensive guide to information security. It should however, assist the Office in deciding on an appropriate course of action if a breach occurs. It is important that the Office has a breach management plan to follow should such an incident occur and that all staff are aware of the personnel to whom they should report an information security incident. Having such a procedure in place will allow for early recognition of the incident so that it can be dealt with in the most appropriate manner. A security breach can happen for a number of reasons, including:-

* Loss or theft of data or equipment on which data is stored (including break-in to the Valuation Office premises.
* Inappropriate access controls allowing unauthorised use, i.e. Disclosure of passwords;
* Equipment failure;
* Human error;
* Unforeseen circumstances such as flood or fire;
* A hacking attack;
* Access where information is obtained by deceiving the Office.

Identification of Data Breach – What an individual should do

1.1 As soon as you find out that personal data (as defined in paragraph 3.2 of the Office's Code of Practice), for which you are responsible, has been compromised, you should immediately report the matter to your team leader/manager and to the Data Protection Officer at cillian.byrnes@valoff.ie. A data breach can occur through the loss of a portable device such as a laptop or a USB key, misaddressing of outgoing mail, a "leak" from the Office, or in any other way,

1.2 The information which you should provide in your report is as follows:

* The date and time that the incident occurred;
* The identity of the person who detected the breach;
* How the breach was discovered;
* Description of the incident, detailing any ICT systems involved, corroborating material such as error messages, log files, etc
* The amount and nature of the data that has been compromised;
* What action (if any) has been taken to inform those affected;
* A chronology of the events leading up to the disclosure;

Containment and Recovery

2.1 Data security breaches will require not only an initial response to investigate and contain the situation but also a recovery plan. Containment involves limiting the scope and impact of the information breach and in doing so, the Data Protection Officer will:

* decide on who should take the lead in investigating the breach and ensure that the appropriate resources are made available for the investigation;
* establish who in the organisation needs to be made aware of the breach and to inform them of what they are expected to do to assist in the containment exercise. For example, this might entail isolating a compromised section of the network finding a lost file or piece of equipment, or simply changing access codes to server rooms, etc.;
* establish whether there is anything that can be done to recover losses and limit the damage the breach can cause;
* will where appropriate, inform the Gardaí.

Risk Assessment

3.1 In assessing the risk arising from a data security breach, the Office will consider what would be the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of materialising, how serious or substantial are they likely to be.

3.2 In assessing the risk, the Office will consider the following points:-

* What type of data is involved?
* How sensitive is it?
* Are there any protections in place (e.g. encryption)?
* What could the data tell a third party about the individual?
* How many individuals are affected by the breach?

Notification of Breaches

4.1 To satisfy Article 33 of the GDPR,In the case of a personal data breach, the Valuation Office shall without undue delay and, where feasible, not later than 48 hours after having become aware of it, notify the personal data breach to the Data Protection Commissioner's Office, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Therefore, if inappropriate release /loss of personal data occurs, it should be reported immediately, both internally and to the Data Protection Commissioner's Office and, if appropriate in the circumstances, to the persons whose data it is.

4.2 The Office will provide specific and clear advice to individuals on the steps they can take to protect themselves and what the Office is willing to do to assist them.

4.3 The Office will also consider notifying third parties such as the Gardaí, bank or credit companies who can assist in reducing the risk of financial loss to individuals. The Office of the Data Protection Commissioner will provide advice upon notification as to the requirement or otherwise, in particular circumstances, to notify individuals.

Evaluation and Response

5.1 Subsequent to any information security breach, a thorough review of the incident will be undertaken. The purpose of this review is to ensure that the steps taken during the incident were appropriate and to identify areas that may need to be improved.

5.2 Any recommended changes to policy and/or procedures will be documented and implemented as soon as possible thereafter.

5.3 The Office will identify a group of people within the organisation who will be responsible for reacting to reported breaches of security.

Action Plan/Steps in Managing a Breach

6.1 The following are the steps to be taken in managing a privacy breach. For each step there is an action required, the individual responsible and the recommended time lines.

Action Required	**Person Responsible**	**Recommended Timelines**
1. Contain the breach	Team Leader and/or staff in area or Office unit where breach occurred.	Immediate
2. Report the breach within the Office	* Team staff (report to team leader) * Management (report to the Data Protection Commissioner, if appropriate)	Same day as breach occurred
3. Designate lead investigator and select breach response team as appropriate	Data Protection Officer	Same day as breach occurred
4. Preserve the evidence	Lead Investigator	Same day as breach occurred
5.Contact Gardaí if necessary	Data Protection Officer	Same day as breach occurred
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach
7.Determine if the breach should be reported to the Data Protection Commissioner	Data Protection Officer in consultation with Management committee	Generally within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Data Protection Officer	Within 2 days of breach
9. Evaluate risks associated with the breach	*Lead Investigator*	*Within 1 week of breach*

10.Determine if notification of affected individuals is required	Data Protection Officer	Within 1 week of breach
11. Conduct notification of affected individual	Data Protection Officer	Within 1 week of breach
12. Contact others as appropriate	Data Protection Officer	As required
13.If required, conduct further investigation into cause and extent of the breach	Lead Investigator	Within 2 to 3 weeks of the breach
14. Review investigative findings and develop prevention strategies	Data Protection Officer in association with relevant line manager and IT management as appropriate.	Within 2 months of breach
15. Implement prevention strategies	Data Protection Officer in association with relevant line manager and IT management as appropriate	Depends on the strategies to be implemented
16. Monitor prevention strategies	Data Protection Officer	Annual Privacy Audit

Appendix 4

Protection of Personal Data by Members of the Management Grades

In compliance with the Code of Practice for the Protection of Personal Data in the Valuation Office, the members of the management grades have adopted the following measures and procedures for the protection of personal data in their custody. Management grades include Senior Managers, Team Leaders, Assistant Principals and Higher Executive Officers or any other person who is responsible for the management of staff in the Valuation Office and Valuation Tribunal.

1. Management are aware of their responsibilities in relation to confidentiality and security when dealing with personal data.

2. Personal information held by management is restricted to PMDS reports in relation to serving members of their staff. Such reports are held only on the manager/team leader's I-drive to which no other staff member has access.

3. No personal data is held on the C-drive (hard drive) of any PC or stored in any other easily accessible network or local drive.

4. Personal information which is electronically transmitted to managers by the Personnel Officer for an official purpose is secured on the I-drive of that manager and retained only for as long as it is officially required.

5. At no time is documentation containing personal data relating to staff left exposed or unattended on desks or other work-tops in Manager's rooms or work areas.

7. If documentation which contains personal data about a member of staff is required for a meeting, this will, at all times, be treated in a confidential manner. It is retained in the custody of the manager at all times and locked away securely when not being used.

8. All files or other documentation which contain the personal data of staff are secured or locked away at the end of each working day.

9. All confidential paper documents containing personal data which is no longer required are shredded by the manager.

10. As a general rule, personal records, whether in paper or electronic format, are kept for no longer than is necessary to carry out official duties.

11. The personal data of staff members who have retired from service or have resigned are shredded if no longer relevant or are transferred to the custody of the Personnel Officer for association with the officer's personal file as appropriate. In the case of staff who transfer, all documents relating to their service are transmitted by Personnel Unit to the new Department or Office in paper and electronic format.

Protection of Personal Data in the Accounts Team

In compliance with the Code of Practice for the Protection of Personal Data in the Valuation Office, the staff of the Accounts Team have adopted the following measures and procedures for the protection of personal data in their custody.

Personal Information - General

- Access to personal information held in the Accounts Team is restricted to the current serving members of the team.
- Files containing such data will not be left unattended on desks and will be locked away in a secure cabinet when not in use.
- All relevant records and files will be secured/locked away at the end of the working day and will only be removed from storage as required. The keys to all presses and storage units will be kept in a secure location.
- At no time will records/files be left unattended on common work-tops or at any desk where staff of other teams/units can observe their contents.
- Accounts documentation which contains personal data will never be brought to meetings in conference rooms or to other team areas.
- Team staff are aware of their responsibilities when dealing with confidential data, emphasising that security is of the utmost importance.
- Records to be kept for no longer than necessary to carry out the work of the Unit.

Accounting Information

- General files relating to the Office Vote, including all accounts and budgetary matters will be locked away at the end of each working day.

Paper Records

- All suspense account paper files containing personal information relating to membership of salary deduction schemes such as insurance, trade union, income tax, social insurance and other similar schemes are to be kept locked in a secure press when not in use.

- All confidential paper documents containing personal data which is no longer required is to shredded in the team area.

- Confidential salary data containing personal details of staff which is being sent to other Government Departments and Offices is to be delivered by hand where practicable. Otherwise, such data may be posted, with the covering envelope marked confidential to the addressee.

- Confidential documents are only sent by fax after contact is made with the person to whom the documents are being sent to ensure delivery only to that person.

- Personal salary records of retired or transferred staff are secured under lock and key and are only accessible by members of the Accounts Team.

Electronic Files

- Confidential personal data relating to staff which is held on the Accounts Network drive is password protected and accessible only by the members of the Accounts Team, the Finance Officer and the Accounting Officer.

- The system ensures that passwords are changed frequently and the Department of Finance is notified when staff should no longer have access to the system.

- No information of a confidential and personal nature is held on the C drive of the office IT system.

Protection of Personal Data in the Personnel and Corporate Services Team

In compliance with the Code of Practice for the Protection of Personal Data in the Valuation Office, the staff of the Personnel and Corporate Services Team have adopted the following measures and procedures for the protection of personal data in their custody.

Corporate Services Unit

Recruitment/Personnel Information

- Access to personal information is restricted to the two staff members of the Unit.
- Files containing such data will not be left unattended on desks and will be locked away in a secure cabinet when not in use.
- All relevant records and files will be secured / locked away at the end of the working day and will only be removed from storage as required.
- At no time will records/files be left unattended on common work-tops or at any desk where staff of other teams/units can observe their contents.

Mobile Phones

- All mobile phones will be Password/Pin code enabled.
- Phones will be securely disposed of, after they have been decommissioned and no longer required for use.
- Hard copy of phone bills will be locked away and access restricted to relevant staff of the unit.
- Electronic bills are password protected by the relevant mobile phone user.

Employment of Disabled Staff

- Access to information relating to disabled staff is restricted to the HEO in Corporate Services who is the designated Disability Officer for the Valuation Office.
- Records are locked away in secure drawer when not in use.
- Records are locked away at the end of each working day.

General Information

- Files and records of a general nature will be locked away at the end of each working day. Keyes are held securely.

The following initiatives will be implemented in 2010 and subsequently

- Records to be kept for no longer than necessary to carry out the work of the Unit.
- Ensure that staff in the team are aware of their responsibilities when dealing with confidential data, emphasising that security is of the utmost importance.
- Paper copies of mobile phone bills to be securely destroyed in accordance with Accounts Branch procedures.

Human Resources Unit

In respect of the personal records of current staff, the following precautions are to be taken at all times.

Paper Records

- All Personal Files and Sick Leave Files are stored in locked cabinets and are only accessible to the staff in the Human Resource Unit and the Personnel Officer.
- Confidential documents in use are locked away each evening before close of business.
- All confidential waste paper is shredded in the team area.
- Confidential data sent to other Government Departments and Offices and to the Offices of the Chief Medical Officer and the Employee Assistance Officer is delivered by hand.
- Confidential documents are only sent by fax after contact is made with the person to whom the documents are being sent to ensure delivery only to that person.
- Confidential documents are delivered internally by hand marked *Private and Confidential*.

Electronic Files

- Confidential data on staff which is held on the Human Resource Management System (HRMS) is password-protected and only accessible by staff in the Unit. The system ensures that passwords are changed frequently and the Department of Finance is notified when staff should no longer have access to the system.
- Most confidential documents are stored on the HR drive which is accessible only by staff in the Unit. No confidential information is held on the C drive of any individual PC.
- The HRMS mailing list is updated as necessary when staff leave the HR Section.

The following procedures are in place for the protection of the personal data of staff who have retired from service and in respect of staff who have transferred to other Departments and Offices.

Paper Records

- All paper files in respect of retired staff are stored in a locked room. Access to those files is limited to the staff in HR.
  - The personal files of all officers who are no longer serving in the Office are stored in line with the Office's HR policy of retention of confidential data.
  - In the case of staff who are transferring to another Government Department or Office, the officer's file is sent on to an identified contact in the new department by hand or registered post.

Electronic Files

- The office holds the electronic data of the retired officers on the HRMS. The electronic record of the transferred staff member is transmitted via the HRMS system to a known contact in the receiving department.

Protection of Personal Data in the Information Technology Team

In compliance with the Code of Practice for the Protection of Personal Data in the Valuation Office, the staff of the Information Technology (IT) Team have adopted the following measures and procedures for the protection of personal data in their custody.

Personal Information - General

- Personal information held in the IT Team is restricted to PMDS reports in relation to serving members of the team. Such reports are held on the team leader's i-drive with no other staff member having access.

- The PMDS data is controlled by Username and Password and is backed up nightly as part of the Office Backup Procedures.

- At no time are paper records/files left unattended on common work-tops or desks where staff of other teams/units can observe their contents.

- Personal data will never be brought to meetings in conference rooms or to other team areas.

- Team staff members are aware of their responsibilities when dealing with confidential data, emphasising that security is of the utmost importance.

- As a general rule, personal records, in whatever format, are to be kept for no longer than necessary to carry out the work of the team.

Paper Records

- All confidential paper documents which might contain personal data which is no longer required is shredded in the team area.

- Confidential documents are only sent by fax after contact is made with the person to whom the documents are being sent to ensure delivery only to that person.

Electronic Files

- Confidential personal data relating to staff which is held on the IT Team Leader's I- drive is password protected and accessible only by the team leader.

- The IT system ensures that passwords are changed frequently.

- No information of a confidential and personal nature is held on the C-drive of the office IT network or stored on any other easily accessible network or local drive.

- The individual members of staff hold their own PMDS role profiles on their personal I-drive which is password protected and not accessible by other staff members.