Department of Health
AN ROINN SLÁINTE

Data Protection - Code of Practice

V3.0: 28/08/2014: Approved by DPC
V3.1: 14/05/2015: Approved by DPC

Table of contents

1. Foreword

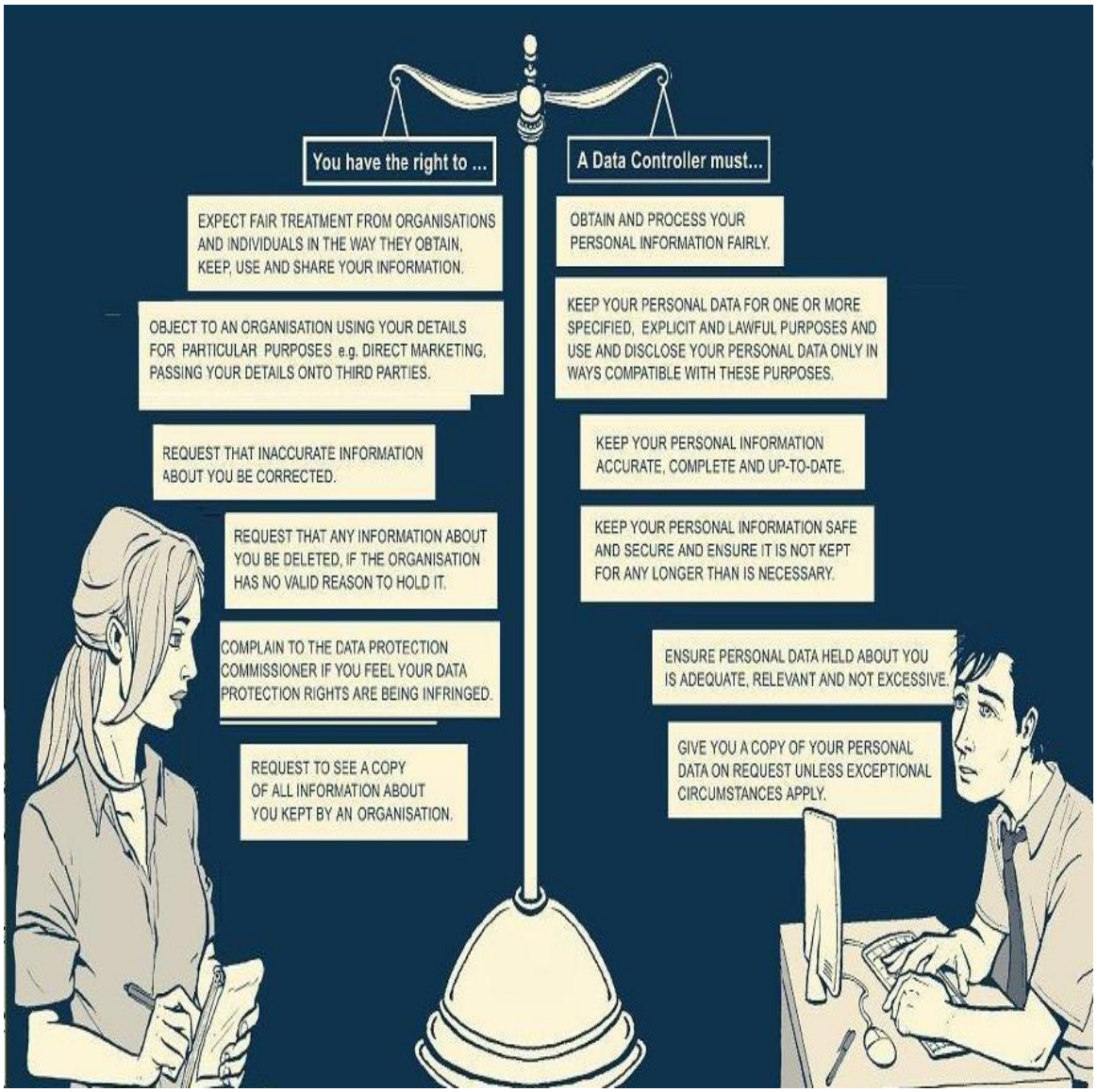
The Department of Health collects, stores and processes personal information belonging to private citizens. See sections 6 and 7 below.

The Data Protection acts of 1988 and 2003 places a burden or "duty of care" on the Department and each of its employees to guard and protect sensitive personal data in our possession from unauthorised access.

Please remember that it is not our data. We may collect it, request it, store it, but it belongs to the private citizen i.e. the data subject.

Data subject's rights are enshrined in these Acts, as are the Department's obligations to protect the personal data of data subjects, as long as it resides in our custody.

Citizen's rights & Department's obligations



2. Introduction

2.1. Following a Government decision of 16th October 2007 that a review should be conducted of systems and procedures to protect the confidentiality of personal data, the Department of Finance undertook such a review and developed a number of recommendations for action. First among them is that:

"*Each Department and agency should have a detailed code of practice on data protection and this should be formally agreed with the Data Protection Commissioner.*"

2.2. This document sets out the Department of Health's code of practice on data protection. It outlines the statutory framework governing these practices, sets out a large number of measures already in place together with additional practices that the Department proposes to adopt in line with the Department of Finance's recommendations.

2.3. The Data Protection Acts of 1988 and 2003 have a significant role to play in supporting the daily operational business of the Department. The aim of this document is to ensure each employee of the Department has an understanding of the concepts of Data Protection and is aware of their own responsibilities. This, in turn, will assist the Department in its compliance as an organisation.

2.4. The Department has recently produced an "Information Security" handbook which issued to all staff of the Department. The handbook, together with the Department's information security' policies, procedures and guidelines are available on Healthnet
@ http://healthnet/informationresources/information_security/
The measures introduced by the Department to strengthen data protection within the Department will assist each employee in understanding and cultivating a habit of data protection in their daily work.

2.5 The Department has drafted an "Information classification and handling" policy document outlining the policies and procedures for classifying and handling all data held by the Department.
Personal data held by the Department is classified as "restricted" and each employee should familiarise themselves with the handling procedures for managing "restricted" data both internally and externally. Section 7 below refers.

2.6 Protecting our data is common sense. We need to ensure that data gathered and processed by the Department is compliant with Data Protection Legislation.
The reading and understanding of these guidelines by all employees of the Department will go a long way towards meeting this requirement.

3. Statutory Framework

3.1. The first legislation that concerns all officers serving in the Department is the Official Secrets Act, 1963, which prohibits the unauthorised disclosure of official information except in accordance with the officer's duties.

3.2. The focus of the Data Protection Acts 1988 and 2003 is to protect the privacy of individuals whose personal data is kept by any organisation. The main provisions of the Acts govern the obtaining, handling, storing, disclosure and processing of personal information. Data subjects also have rights under these Acts to access - and have corrected - information held concerning them.

3.3. When addressing the provisions of the Data Protection Acts, it is also useful to mention the Freedom of Information Acts, 1997 and 2003, which contain access provisions that sometimes need to be considered in conjunction with the Data Protection Acts. Section 28 of the FOI Act concerns access to personal information, and any request under this provision should also be treated under the Data Protection Acts and vice versa, to ensure that requesters are accorded their full range of rights.

4. Classification and handling guidelines

Information Classification Scheme:
All information generated by or for the Department in written, verbal, electronic, or any other form, must be classified according to its level of confidentiality, and in adherence to the Department's "information classification and handling" policy.

i.e. Information must be classified using the following classification definitions.

Classification	Definition
Confidential	Information that could seriously damage the Department if lost or made public.
Restricted	Information whose disclosure would cause the Department to be in breach of legal or regulatory requirements.
Internal	Information whose disclosure would embarrass or inconvenience line management but is unlikely to impact on customer relationships
Public	Information whose public disclosure would benefit or have no impact on the Department.

5. Definitions

Personal data in the context of the Data Protection Acts 1988 and 2003, means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the Data Controller.

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 or trade union membership.

Data Processor is a person who processes personal information 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 Act places responsibilities on such entities in relation to their processing of the data

Data Controller a person who (either alone or with others) controls the contents and use of personal data. The Department's Data Controller for the purpose of these Acts is the Secretary General of the Department.

Data Subject - An individual who is the subject of personal data.

Access Request is where a person makes a request to the Department for the disclosure of their personal data under section 4 of the 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.

Data - Information in a form that can be processed. It includes **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 Processing - Performing any operation or set of operations on data, including:

- Obtaining, recording or keeping the data;
- Collecting, organising, storing, altering or adapting the data;
- Retrieving, consulting or using the data;
- Disclosing the data by transmitting, disseminating or otherwise making it available;
- Aligning, combining, blocking, erasing or destroying the data.

Relevant Filing Systems - Any set of information 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..

6. Registration

The Department of Health is registered as a Data Controller under the Data Protection Acts 1988 and 2003. The Department provides annually, a list of personal data holdings and data exchanges made under national legislation, EU and other binding international agreements to the Office of the Data Protection Commissioner. Further information on the types of information processed by the Department of Health and disclosees can be viewed on:-
https://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/display.asp?ID=0479%2FA

7. Examples where the Department holds personal data

Job application forms, registration forms for programmes or schemes, membership/employees of boards, licences i.e. animal experimentation and other, CV's of health professionals, details of legal cases, formal complaints , appeals, appellant cases. Appointments e.g. under section 70 of the Health Act 2007, legal settlement payments , Health Repayment Scheme, PQ, FOI and Min Rep databases, records relating to tribunals/ commissions/inquiries/High Court data, notifications under the Medical Practitioners Acts. Various contact databases, implementation groups and committees, deaths of children in care. Public consultation participant details.

A comprehensive list of personal data held by the Department, and the purposes for which it is held is available @
https://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/display.asp?ID=0479%2FA

8. Rules and Obligations

The main principles of the Data Protection Acts are summarised in the following eight Data Protection Principles identified by the Data Protection Commissioner:

1) **Obtain and process information fairly**
2) **Keep it only for one or more specified, explicit and lawful purposes**
3) **Process it only in ways compatible with the purposes for which it was given to you initially**
4) **Keep it safe and secure**
5) **Keep it accurate, complete and up-to-date**
6) **Ensure that it is adequate, relevant and not excessive**
7) **Retain it for no longer than is necessary for the purpose or purposes**
8) **Give a copy of his/her personal data to an individual, on request**

The Data Protection provisions or RULES apply to **ALL** personal data held by the Department.

The Acts also provide that a "duty of care" is owed to data subjects i.e. private citizens, which means that those controlling or processing the data should take care that their activities do not cause damage or distress to the people concerned by, for example, maintaining inaccurate information on our files, or disclosing personal data to someone who is not entitled to this data.

The Department obtains and holds data to administer its functions. Staff are provided with access to that data in order to do their jobs. Under no circumstances should personal data be accessed without a direct business requirement. Confidential customer information must never be discussed with or disclosed to any unauthorised third party, either internal or external.

9. Data Protection rules

The Data Protection Acts of 1988 and 2003 stipulate a set of eight rules that each employee of the Department of Health must adhere to when processing personal data.

Rule 1. Obtain and process data fairly and lawfully

Personal data is obtained fairly if the data subject, is at the time the personal data is being collected made aware of.

1 the identity of the Data Controller
2 the purpose for which the Department is collecting the data at the point of collection
3 the person or categories of persons to whom the data may be disclosed
4 any other information which is necessary so that processing may be fair

The Department is committed to treating the information given to us in confidence and ensure that it will not be used or disclosed except as provided for by law, and will collect no more information than is necessary.

Rule 2. Keep it only for one or more specified, explicit and lawful purposes

The Department may only keep data for a purpose/s that are specific, lawful and clearly stated and the data should only be processed in a manner compatible with the purpose.

An individual has a right to question the purpose for which the Department holds his/her data and the Department must be able to identify that purpose.

The Department holds information for a variety of purposes. Much of this information is held for statutory compliance reasons, while other information is obtained, collected and held in the context of the administration of the Department. e.g. personnel files of all employees, payroll, HR, travel and subsistence claims etc.

Electronic or paper forms requesting personal data issued from the Department will state what the data will be used for and who will have access to the data.
Any secondary or future uses for the data, which might not be obvious to individuals, will be brought to their attention at the time of obtaining personal data. Individuals will be given the option of saying whether or not they wish their data to be used in these other ways. If the Department has data about people and wishes to use it for a new purpose (which was not disclosed and perhaps not even contemplated at the time the data was collected), individuals will be given an option to indicate whether or not they wish their data to be used for the new purpose.

Rule 3. Disclosing Personal Data

Personal information obtained by the Department of Health for a particular purpose may not, in general terms, be used for any purpose other than that for which it was Obtained.

Personal data should only be disclosed in ways that are necessary or compatible with the purpose for which it is held.

Staff may not disclose any personal data to any third party without the consent of the data subject (see exceptions below).

The Act places serious responsibilities on every employee of the Department not to disclose data in relation to any individual who is not entitled by law to receive it.

Personal data should not be disclosed to work colleagues unless they have a legitimate interest in the data in order to fulfil official duties.

Personal data held by the Department is classified as "restricted" and each employee should familiarise themselves with the handling procedures for managing "restricted" data both internally and externally.

For the purposes of the Acts, processing of personal data by contractors on behalf of the Department does not constitute disclosure. However, such transfers are subject to appropriate contractual agreements including provisions relating to data protection with specific security and disposal/retention arrangements. Department staff are instructed through operating procedures in relation to transfers of data and responsibilities of contractors when handling Department data.

A comprehensive list of disclosees of personal data held in the Department is made annually to the Data Protection Commissioner and can be viewed @ https://www.dataprotection.ie/ViewDoc.asp?fn=/documents/register/display.asp?ID=0479%2FA

Exceptions:
Permitted disclosures of personal data

Personal data can be disclosed without the express written consent of the data subject in the following circumstances:

- to the data subject or to a person acting on his/her behalf
- at the request or with the consent of the data subject or a person acting on his/her behalf
- where the data subject has already been made aware of the person/organisations to whom the data may be disclosed
- required by law or a court order
- required for legal advice or legal proceedings, where the person making the disclosure is a party or witness
- required for the purposes of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing moneys due to the State, a local authority or a health board
- authorised for safeguarding the security of the State (if it is in the opinion of a member of the Garda Siochana not below the rank of chief superintendent or an officer of the Permanent Defence Forces not below the rank of colonel)
- required urgently to prevent injury or damage to health or serious loss of or damage to property
- required to protect the international relations of the State.

Rule 4. Keep it safe and secure

The Department must provide "appropriate" security measures to protect personal data from unauthorised access when in use and in storage or in transit and must protect it from inadvertent destruction, amendment, loss, disclosure, corruption or unlawful processing.

In compliance with this requirement the Department has put in place physical and technical security measures to protect the confidentiality of personal data. Including, inter alia;

Personal data obtained and held by the Department is classified as "restricted". Each employee should familiarise themselves with the handling procedures for managing "restricted" data both internally and externally and in accordance with the Department's Information classification and handling policy and in compliance with the Data Protection Acts.

Access to personal information is restricted to authorised staff on a "need-to- know" basis and in accordance with the Department's Information classification and handling policy and in compliance with the Data Protection Acts.

Staff are reminded to familiarise themselves with the Department's "Information Security" handbook and the information security policies, procedures and guidelines when accessing personal data on computer systems belonging to the Department i.e. Healthnet link @ http://healthnet/informationresources/information_security/

Electronic personal data is protected by stringent access controls, passwords, access logs, audit logs, back-ups etc.

Screens, print-outs, documents and files showing personal data should not be visible to unauthorised persons.

Appropriate facilities are in place for disposal of confidential waste.

Personal manual data should be held securely in locked cabinets, locked rooms, or rooms with limited access.

Special care must be taken if storing personal data on mobile computing and storage devices. Where deemed essential, the data must be encrypted and a record kept of the nature and extent of the data and why it is being stored on a portable device. Arrangements should be in place to fully delete the data on the portable device when it is no longer being used. The Department's laptop and mobile media policy refers.

Special care must be taken if transferring personal data electronically. Where deemed essential staff must ensure that personal data being transferred is encrypted i.e. by using the Department's secure email system.

Appropriate data protection and confidentiality clauses must be specified in any arrangements with data processors of personal data on the Department's behalf, including –

- the conditions under which data may be processed.
- the minimum security measures that the data processors must have in place.
- mechanisms or provisions that will enable the data controller to ensure that any data processor is compliant with the security.

- practices which include a right of inspection or independent audit.
- retention/disposal: in general the retention periods for data within the Department are subject to the legislative provisions pertaining to the area involved.

Staff are not to disclose personal security passwords to anyone within the department who does not have a legitimate need to know the information in the normal course of their duties, or to anyone outside the Department of Health, unless authorised through the proper mechanisms and in accordance with the relevant requirements (e.g. Non Disclosure Agreements, contracts, etc.).

While ultimately the Data Controller is responsible in law for the security of personal information it is a responsibility shared with every officer in the Department.

Rule 5. Keep it accurate, complete and up-to-date

Data Controllers must keep data subject's data accurate, complete and up-to-date.

Once the Department is informed of any changes to personal data it is imperative that the data is amended accordingly.

To comply with this rule the Department must ensure that:

1 clerical and computer procedures are adequate to ensure high levels of data accuracy,
2 the general requirement to keep personal data up-to-date has been fully implemented,
3 appropriate procedures are in place, including periodic review and audit, to ensure that each data item is kept up-to-date.
4 procedures are in place to ensure personal data held is accurate, including reviewing records on a regular basis, identifying areas where errors are most common and providing guidelines to staff on eliminating errors.

Section 6 of the Acts gives a person a right to seek to have their personal data amended or erased where it can be shown that it is incorrect.

Rule 6. Ensure that it is adequate, relevant and not excessive

Personal data obtained and kept within the Department must be minimum amount of personal data needed for the specified purpose, and no more.

The Department may not collect or keep personal information that is not needed, or "just in case" a use can be found for the data in the future. Informally this is called the "fair obtaining" rule.

To comply with this rule each employee should ensure that the information held is:

1 adequate in relation to the purpose/s for which it is kept,
2 relevant in relation to the purpose/s for which it is kept,
3 not excessive in relation to the purpose/s for which it is kept.
4 subject to periodic review and audit, to ensure that each data item is adequate, relevant and not excessive.

Rule 7. Retention and Disposal of personal data

Data should not be kept for any longer than is necessary for the purpose for which it was collected and should not be subject to further processing that is not compatible with that purpose.

In general the retention period for data within the Department is subject to the legislative provisions pertaining to the area involved.
The Department is legally obliged to seek authorisation from the Director of the National Archives in relation to the destruction of Department records that are subject to that legislation. The Departments Data Retention policy also refers.

To ensure compliance with this rule each employee should ensure that:

- personal data is regularly purged and that personal data is not retained any longer than necessary.
- personal data should be categorised as essential or non-essential
- all electronic and manual data is retained in line with the Department's records management protocol on data retention, which outlines retention periods for categories of personal data kept by the Department.

Personal data should be disposed of **securely** when no longer required. The method should be appropriate to the sensitivity of the data.

Shredding or incineration is appropriate in respect of manual data; and reformatting or overwriting in the case of electronic data.

Rule 8. Rights of Data Subjects

(give a copy of his/her personal data to an individual, on request)

The Data Protection Acts provide for the right of access by the data subject to his or her personal information.

Accordingly, if an employee receives an access request under section 4 of the Data Protection Acts it should be brought immediately to their line manager.

Under the Data Protection Act, there is a nominal fee of €6.35 payable, and this should be included with any access requests made under the Act. The applicant should provide the necessary details to help identify and locate all the information kept about him/her

Where a request is made to the Department by, or on behalf of, a person seeking access to their own personal information under the Freedom of Information Act, this request should be considered in conjunction with the Data Protection Acts.

Data subjects, who make a valid request in writing, have, *inter alia,* the following rights under the Data Protection Act, within 40 days of so requesting:

1 to be informed whether the Department holds data relating to them.
2 to be told the category, details, purpose, disclosees and, unless contrary to the public interest, the source of the information.
3 to be given a copy of the data being kept about him/her.
4 to be given a copy of any data held in the form of opinions, except where such opinions were given in confidence
5 to be told the logic of any decision significantly affecting them, where the decision was based solely on the outcome of automatic processing of the data.

Some of these rights are qualified by other provisions of the Act. Access requests under the Data Protection Act are co-ordinated by the FOI Unit in much the same way as Freedom of Information requests; however, responses to DP requests should be submitted via the FOI Unit to the Data Controller for final decision and issue of reply.

In response to an access request the Department must:

- supply the information to the individual promptly and within 40 days of receiving the request,
- provide the information in a form which will be clear to the ordinary person, e.g. any codes must be explained in ordinary language.
- Where an access request is being **refused** the reasons for its refusal must be clearly outlined (as per exemptions in Sections 4 and 5 of the Data
- Protection Acts)

Information about a third party can only be disclosed if the third party has given consent to the person making the request.

The Department's website @ http://www.health.gov.ie/data-protection/ explains how individuals can seek access to their own personal data in the Department of Health.

Applying for Access to Personal Data
Requests for personal data should be made in writing to:

The Data Controller
Department of Health
Hawkins House
Dublin 2

10. Responsibilities of Data Controller

Ultimate responsibility for the compliance of each employee of the Department with the Data Protection Acts rests with the Department's Data Controller, who is currently the Principal Officer with responsibility for ICT.

The Data Controller is responsible for:

- overseeing the management of data protection matters within the Department;
- ensuring that reporting lines exist to allow other employees of the Department to raise matters relating to data protection at a senior level;
- managing the Department's statutory obligations in respect of the Data Protection Acts including: compliance with the Data Protection Principles, registration with the Data Protection Commissioner and securing individuals rights under the Acts;
- maintaining an up to date knowledge of Data Protection legislation and general developments in other relevant areas (e.g. Freedom of Information Act) and ensuring that this Data Protection code of practice along with other related policies and procedures is disseminated and adhered to throughout the Department;
- promoting data protection awareness through training, policy development, advice and guidance, ensuring that operating rules and general policy guidance in support of these guidelines and all matters relating to the Acts are available to all staff;
- ensuring information and systems comply with the Data Protection Principles and that appropriate security arrangements exist to protect data, including where

necessary, that suitable contracts are drawn up relating to the processing of data held for the Department by third parties;
- investigating and resolving complaints made in relation to personal data and assisting, where appropriate, in the investigation of disciplinary and criminal matters relating to unlawful disclosure of data;
- providing for liaison on all data protection matters between The Department and the Data Protection Commissioner.
- reporting all incidents where personal data has been put at risk to the Office of the Data Protection Commissioner, within two working days of becoming aware of an incident.

11. Responsibilities of all Department staff

All staff of the Department are provided with Data Protection and Information Security awareness training.
The Department also ensures that information to allow staff and managers to fully comply with this Code of Practice and the Department's data security policies is provided on the Department's Intranet.

It is the responsibility of every staff member to:

- To be familiar with and to comply with the principles of Data Protection and to follow the Department's policy as stated in this Data Protection code of practice.
- To report any suspected breach of personal data to the Department's Data Controller or Information Security manager.
- To ensure that all data accessed, managed and controlled as part of their daily duties is done so in accordance with the Data Protection Acts and this Data Protection code of practice .
- To be aware that breaching the Data Protection Rules may constitute an offence under the Data Protection Acts, which risks exposing individual staff members and the Department to litigation from an injured party.
- To be accountable in relation to all data processed, managed and controlled by them during the performance of their duties in the Department; this accountability extends to former employees of the Department too;
- To be familiar with the Department's information security' policies, procedures and guidelines.
- To follow the Department's classification and handling policy when categorising data.

12. Audits of procedures

To ensure the quality of data retained by the Department, and that access to and usage of such data is appropriate within the terms of this code; the Department's Internal Audit Unit will conduct examinations and reviews of Data Protection procedures as part of their ongoing examination and review process.

Risks associated with the storage, handling and protection of personal data are included in the Revenue's risk register and risk assessments should take place as part of the Department's risk strategy.

Furthermore, external audits of all aspects of Data Protection within the Department may be conducted on a periodic basis by the Office of the Data Protection Commissioner

13. Enforcement of Data Protection legislation

The Department's Code of Practice on Data Protection can be summed up as follows:

(a) Access to business and personal information is authorised only in circumstances where there is a clear official business reason requiring such access; and
(b) Any unauthorised access constitutes a serious breach of discipline and will be dealt with accordingly.

Where complaints are made to the Department by data subjects in relation to the handling or disclosure of their personal information, these will be investigated by the Data Controller's team and reported to the Department's Information Security Forum for decision as to any action to be taken on foot of the complaint. The complainant should be advised of the outcome of the investigation.

Where employees of the Department, in the normal course of their duties, become aware that an individual may be breaching the Acts, or have committed or are committing an offence under the Acts, they should report the matter to their line manager and to the Department's Data Controller.

Where unlawful disclosure of personal information is known to have taken place, the Department's policy is to notify and apologise to the data subject, where possible, without delay, and to notify the Data Protection Commissioner, within two working days of becoming aware of the incident. Any discovery of such a breach of the Act should be followed up with a security audit of the business area in question.

Officers in breach of Data Protection privacy provisions may face disciplinary proceedings under the Civil Service Disciplinary Code.

Officers should note that the Data Protection Commissioner has a wide range of enforcement powers to assist in ensuring that the principles of data protection are being observed, including:

- serving legal notices compelling Data Controllers to provide information needed to assist his enquires, or compelling a Data Controller to implement one or more provisions of the Acts.
- investigate complaints made by the general public or carry out investigations proactively. He may, for example, authorise officers to enter premises and to inspect the type of personal information kept, how it is processed and the security measures in place. Staff must cooperate fully with such officers.

14. Notifying security breaches

A data breach can be identified as any event which results in the integrity or security of personal data being compromised. Such a breach can occur for a number of reasons including loss or theft of electronic equipment on which personal data is stored, equipment failure, human error, and a successful hacking attack.

At the time of writing there is no legal obligation to notify the Commissioner of a data breach. However, on July 7th, 2010 the Data Protection Review Commissioner approved a code of practice which recommends that Data Controllers notify both data subjects and the Commissioner's office of data security breaches.

Code of practice for data security breaches:

1. The Data Protection Acts 1988 and 2003 impose obligations on data controllers [1] to process personal data entrusted to them in a manner that respects the rights of data subjects to have their data processed fairly (Section 2(1)).Data controllers are under a specific obligation to take appropriate measures to protect the security of such data (Section 2(1)(d)).This Code of Practice does not apply to providers of publicly available electronic communications networks or services.[2]

2. This Code of Practice addresses situations where personal data has been put at risk of unauthorised disclosure, loss, destruction or alteration. The focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.

3. Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, the data controller must give immediate consideration to informing those affected.[3] Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána, financial institutions etc.

4. If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it,the data controller may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures(such as encryption) were of a high standard.

5. All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to the relevant data controller as soon as the data processor becomes aware of the incident.

6. All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner as soon as the data controller becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include

sensitive personal data or personal data of a financial nature.[4]In case of doubt- in particular any doubt related to the adequacy of technological risk-mitigation measures - the data controller should report the incident to the Office of the Data Protection Commissioner.

7. Data controllers reporting to the Office of the Data Protection Commissioner in accordance with this Code should make initial contact with the Office within two working days of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact may be by e-mail (preferably), telephone or fax and must not involve the communication of personal data. The Office of the Data Protection Commissioner will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

8. Should the Office of the Data Protection Commissioner request a data controller to provide a detailed written report of the incident, the Office will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:
    - the amount and nature of the personal data that has been compromised;
    - the action being taken to secure and / or recover the personal data that has been compromised;
    - the action being taken to inform those affected by the incident or reasons for the decision not to do so;
    - the action being taken to limit damage or distress to those affected by the incident;
    - a chronology of the events leading up to the loss of control of the personal data; and
    - the measures being taken to prevent repetition of the incident.

9. Depending on the nature of the incident, the Office of the Data Protection Commissioner may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where a data controller has not already done so
If necessary, the Commissioner may use his enforcement powers to compel appropriate action to protect the interests of data subjects.

10. Even where there is no notification of the Office of the Data Protection Commissioner, the data controller should keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the data controller did not consider it necessary to inform the Office of the Data Protection Commissioner. Such records should be provided to the Office of the Data Protection Commissioner upon request.

11. This Code of Practice applies to all categories of data controllers and data processors to which the Data Protection Acts 1988 and 2003 apply.