An Roinn Cosanta
Department of Defence

Department of Defence

Data Protection Policy

July, 2013

Foreword

This policy sets out the requirements of the Data Protection Acts 1988 and 2003, when collecting, handling, storing and destroying personal data and sensitive personal data, the steps involved in responding to requests for such data and the contact details for those individuals in the Department with designated responsibility for Data Protection. The policy also provides guidelines for the management of any data security breaches.

The scope of the policy applies to all staff of the Department, both permanent and temporary, and to staff working on a contract basis for the Department and others who are authorised to access personal data held by the Department.

Staff should familiarise themselves with Data Protection issues set out in this Policy Document and are required to sign the Acknowledgement on page 35.

Depending on your location, the signed acknowledgement should be returned to one of the following:

Newbridge: Clair Gaffney, Data Protection Team, Facilities Management.

Renmore: Sheila Burns, HR Branch.

Roscrea: John Fitzpatrick, Civil Defence Admin

Heads of Branches are required to ensure that all staff within the Department comply with the provisions of the Data Protection legislation in relation to personal data obtained and held on behalf of any individual. Furthermore, they are required to review procedures within their Branches to ensure compliance with this policy as part of the annual Business Planning process.

This document will be updated as required to include any changes or further amendments to Data Protection legislation.

Further information is available on the website of the Office of the Data Protection Commissioner on www.dataprotection.ie

Data Protection Team
Facilities Management

Introduction from the Secretary General

Data (including information and knowledge) is essential to the administrative business of the Department. There is a balance to be struck between an individual's right to privacy and the legitimate business requirements of the Department. We all owe a duty of care to citizens, on whose behalf we hold personal data, that in obtaining, processing, retaining and destroying such data, we do so professionally and in accordance with the legal provisions laid down in the Data Protection Acts, 1988 and 2003.

This document gives operational effect to Data Protection Legislation and sets out clearly the principles of data protection and the responsibilities of staff in relation to the implementation of these principles.

Protecting our data is common sense. We need to ensure that data gathered and processed by the Department is compliant with Data Protection Legislation.

Michael Howard
Secretary General

May, 2013

I N D E X

		Page
Part 1:	**Rights and Responsibilities of Key Parties**	**5**
Part 2:	**Data Protection Rules**	**11**
Part 3:	**Subject Access Requests**	**15**
Part 4:	**Exceptions to provisions of the Data Protection Acts**	**17**
Part 5:	**Audits**	**20**
Part 6:	**Data Security Breaches**	**21**

A P P E N D I C E S

Appendix I	***Key Terms and Definitions in the Data Protection Field***	**26**
Appendix II	***Personnel in the Department with a designated responsibility for Data Protection***	**29**
Appendix III	***Subject Access Request Form***	**30**
Appendix IV	***Sample Acknowledgement letter of receipt of Subject Access Request***	**33**
Appendix V	***Submission to Data Controller***	**34**
Appendix VI	***Acknowledgement***	**35**

INTRODUCTION

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 Department staff must comply with the provisions of the Data Protection Acts when collecting and storing personal data. This applies to personal data relating to both employees of and individuals who interact with the Department.

The 1988 Act refers to manual data only while the 2003 Act covers both automated and manual data. A copy of both Acts is available on the DNET under "*Freedom of Information and Data Protection"*.

1. Rights and Responsibilities of Key Parties

1.1 Rights of Data Subjects

The Data Protection Acts 1988 and 2003 confer a number of rights in respect of individuals on whose behalf personal or sensitive personal data is held:-

- A person has the right to access personal data held on computer or in a manual filing system which identifies them.
- A person has a right to be given, on request, a **description** of the data held about them and the purposes for which it is kept and this **description** must be provided no later than **21 days** from receipt of this request.
- The person is also entitled to request a **copy** of the personal data held, no later than **40 days** from the receipt of this request. This is normally called a Subject Access Request (SAR). Under the terms of the legislation, the Data Controller may choose to impose a fee, not exceeding €6.35, which is payable to the Department by the Data Subject.
- If the data held about an individual is inaccurate, that individual has the right to have the data corrected or rectified. In some cases, the individual may request that the data be erased. For example if the organisation/person holding the data has no good reason for retaining it, or if the data was originally obtained unfairly, or without the Data Subject's consent.
- A person may request to prevent data on them from being used for certain purposes particularly if it was originally obtained for other purposes.
- A person who suffers damage through the mishandling of personal or sensitive personal data may be entitled to seek compensation through the courts of law.

1.2 Responsibilities of the Data Controller

Data Controllers are responsible for controlling the content and use of personal data. All responses to requests for copies of personal data or other requests submitted under the terms of the Data Protection Acts must be submitted to, and examined by the Department's Data Controller, Assistant Secretary, Des Dowling before being issued to the Data Subject.

The Data Controller will also decide on the appropriate action to be taken in the event of a data security breach.

Under the Data Protection Acts 1988 and 2003, certain categories of Data Controllers and Data Processors are obliged to register with the Data Protection Commissioner (DPC) The register is in the public domain and is available on the DPC website at www.dataprotection.ie

1.3 Responsibilities of Employees

All employees have a duty to ensure compliance with the principles of Data Protection and undertake to follow the provisions of this policy. All employees are charged with the responsibility for ensuring that all data accessed, retained, processed and/or controlled by them as part of their daily duties, is done so in accordance with the Data Protection Acts and this policy. Breaches of the rules in this policy may result in disciplinary action.

1.4 Responsibilities of Heads of Branches

Heads of Branches are responsible for ensuring that staff in their area are aware of, and understand the provisions of this policy document and comply fully with the 8 Rules of Data Protection in relation to obtaining, using and retaining of all personal data. **See Section 2.**

Heads of Branches are also responsible for co-ordinating responses to requests made under the Data Protection Acts received in their Branch and must submit the response to the Data Controller for approval before issuing to the requester. **See Appendix V.**

In the event of a data security breach within their area, Heads of Branches are required to submit a report to the Data Controller and Data Protection Officer. **See Section 6.**

1.5 Responsibilities of the Data Protection Team and the Data Protection Officer

The Data Protection Team within Facilities Management (John Thornton, Clair Gaffney, Maura Flanagan and Carol Bourke) is responsible for ensuring that the Department's Data Protection Policy is made available to all staff, updating the policy as and when required and monitoring compliance with the provisions of the policy.

The Data Protection Officer is John Thornton. John will liaise with Heads of Branches regarding the continued effectiveness of data protection measures within their respective areas and will provide assistance and guidance, if required, to Branches when requests for information on personal data (Subject Access Requests, (SAR)) are received. If a Data Protection breach occurs the Head of Branch should notify the Data Controller and Data Protection Officer immediately and follow the steps outlined in **Section 6.**

1.6 Responsibilities of Data Protection Commissioner

The Data Protection Commissioner, Mr. Billy Hawkes, is responsible for ensuring that peoples' rights under Data Protection legislation are respected and that the persons who keep personal information on computer or in manual format meet their responsibilities. To assist the Commissioner in exercising these functions, he is assigned certain important powers under the Data Protection Acts, 1988 and 2003 and under the Electronic Communications Regulations, S.I. 336 of 2011.

1.6.1: Investigations by the Data Protection Commissioner

Under Section 10 of the Data Protection Acts, 1988 and 2003, the Commissioner must investigate any complaint(s) which he receives from individuals who feel that personal information about them is not being treated in accordance with the Act, unless he is of the opinion that such complaints are "frivolous or vexatious".

When the Department receives a complaint from the Data Protection Commissioner, the Data Controller must acknowledge receipt of the complaint immediately and include the name of the officer appointed to investigate the complaint. A final reply must issue as soon as possible.

With regard to complaints of potential breaches of the Data Protection Acts, the Commissioner is obliged to seek an amicable resolution to the complaint in the first instance.

Where a successful resolution to the matter is not possible, the Commissioner may make a Decision on the complaint and this Decision can be appealed to the Circuit Court.

The Commissioner may also launch investigations on his own initiative, where he is of the opinion that there might be a breach of the Act, or where he considers it appropriate in order to ensure compliance with the Acts. In practice, the investigations to ensure compliance take the form of ***'Privacy Audits'***. The Data Controller will get advance notice of the Privacy Audit.

The primary aim of the ***'Privacy Audit'*** is to assist in improving data protection practices and it is only in the event of serious breaches being discovered or failure of the Data Controller to implement recommendations that further sanctions would be considered by the Data Protection Commissioner.

1.6.2: The Commissioner's Power to Obtain Information

Under Section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require any person to provide him with whatever information the Commissioner needs to carry out his functions, such as the pursuit of an investigation. The Commissioner exercises this power by providing a written notice, called an ***'Information Notice'***, to the person.

A person who receives an Information Notice has the right to appeal it to the Circuit Court.

Failure to comply with an Information Notice without reasonable excuse is an offence. Knowingly to provide false information or information that is misleading in a material respect, in response to an Information Notice is an offence. No legal prohibition may stand in the way of compliance with an Information Notice. The only exceptions to compliance with an Information Notice are (i) where the information in question is or was, in the opinion of the Minister for Justice, Equality and Law Reform, or in the opinion of the Minister for Defence, kept for the purpose of safeguarding the security of the State, and (ii) where the information is privileged from disclosure in proceedings in any Court.

1.6.3: The Commissioner's Power to Enforce Compliance with the Act

Under Section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a Data Controller or Data Processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Acts, 1988 and 2003. Such steps could include correcting

the data, blocking the data from use for certain purposes, supplementing the data with a statement which the Commissioner approves, or erasing the data altogether. The Commissioner exercises this power by providing a written notice called an *'Enforcement Notice'* to the Data Controller or Data Processor. A person who receives an Enforcement Notice has the right to appeal it to the Circuit Court.

It is an offence to fail or refuse to comply with an Enforcement Notice without reasonable excuse.

1.6.4: The Powers of "Authorised Officers" to Enter and Examine Premises

Under Section 24 of the Data Protection Acts, 1988 and 2003 and under Regulation 19 of S.I. 336 of 2011 the Data Protection Commissioner may appoint an "Authorised Officer" to enter and examine the premises of a Data Controller or Data Processor to enable the Commissioner to carry out his functions, such as to pursue an investigation.

The Authorised Officer has the power to:

- enter the premises and inspect any data equipment there.
- require the data controller, data processor or staff to assist in obtaining access to data, and to provide any related information.
- inspect and copy any information.
- require the data controller, data processor or staff to provide information about procedures on complying with the Act, sources of data, purposes for which personal data are kept, persons to whom data are disclosed, and data equipment on the premises.

It is an offence to obstruct or impede an Authorised Officer; to fail to comply with any of the requirements set out above; or knowingly to give false or misleading information to an Authorised Officer.

1.6.5: Prosecution of offences under Data Protection Acts and under S.I. 336 of 2011

Section 30 of the Data Protection Acts provides that the Commissioner may bring summary proceedings for an offence under the Acts. The Commissioner also has the power to prosecute offences in relation to offences under S.I. 336 of 2011 (Electronic Communications Regulations).

1.6.6: Data Protection Register

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. For more details on the role and responsibilities of the Data Protection Commissioner, please go to www.dataprotection.ie

2. Data Protection Rules

There are 8 rules:-

2.1 Obtain and process Data fairly.

2.2 Keep the Data only for one or more specified, explicit and lawful purposes.

2.3 Use and disclose only in ways compatible with the purposes for which the Data was initially obtained.

2.4 Keep Data safe and secure.

2.5 Keep Data accurate, complete and where necessary, up-to-date.

2.6 Ensure that Data is adequate, relevant and not excessive in relation to the purpose for which it was obtained.

2.7 Retain Data for no longer than is necessary for the specified purpose(s).

2.8 Give a copy of his/her Personal Data on request from the Data Subject and, where required and necessary, correct, block or erase the Data requested by the individual.

2.1: Obtain and Process Data Fairly

The Department must collect and use information fairly. Forms issued from the Department requesting personal data must state what the data will be used for and who will have access to it.

Secondary or future uses of the data should also be brought to the attention of the data subject at the time the data is being collected. The individuals should then be given the option of stating whether or not they wish their data to be used for these particular purposes.

If the Department has data and wishes to use it for other purposes not previously identified, it must first obtain the permission of the data subject, unless the particular purpose is set out in law and does not require the sanction of the data subject.

2.2: Keep the Data only for one or more specified, explicit and lawful purposes

Data can only be held by a data controller or processor for clear and lawful purposes. Personal data therefore must be obtained and processed in accordance with the legislation. It is unlawful to routinely and indiscriminately collect personal data.

2.3: Use and disclose only in ways compatible with the purposes for which the Data was initially obtained

Personal data obtained for a specific purpose or purposes can only be used for these purposes and the Department cannot divulge personal data to a third party unless it is compatible with the purpose or purposes for which it was obtained.

2.4: Keep Data safe and secure

It is the responsibility of each Head of Branch to ensure that all personal data held in that Branch is kept safe and secure. This may involve physical measures including safes, locked cabinets and tambour units as well as IT systems which are password-protected.

In addition, each Head of Branch is responsible for ensuring that access to such data is restricted to those staff who have a role in processing the information.

Measures to protect the data should include:

- Computers to be locked when staff leave their workstations
- Access to information is restricted to authorised staff
- Paper files to be locked away when not being used
- Portable electronic devices have strong encryption facilities
- Formal procedures in place by Facilities Management for the allocation of swipe access cards to authorised personnel only. Such cards to be disabled by Facilities Management when no longer required.

2.5: Keep Data accurate, complete and where necessary, up-to-date

Heads of Branch are required to oversee periodic checks of personal data held as part of the annual Business Planning process to ensure that it is accurate and up-to-date. Data subjects have the right to have any inaccurate personal data amended or erased.

2.6: Ensure that Data is adequate, relevant and not excessive in relation to the purpose for which it was obtained

Personal data held by the Department should be enough to enable that particular Branch to achieve its purpose and no more. The Department must not collect or keep personal information that is not required for a specific purpose. Forms used to obtain the personal information must state clearly what the data is to be used for. Using such information for other purposes is unlawful if consent from the data subject has not been obtained.

2.7: Retain Data for no longer than is necessary for the specified purpose(s)

It is a key requirement of Data Protection legislation that personal data collected for one purpose cannot be retained once that initial purpose has ceased. Equally, as long as personal data is retained the full obligations of the Acts attach to it.

The Department is required to be clear about the length of time for which data will be kept and the reason why the data is being retained. Data should never be kept on a 'just in case' basis.

As part of the Department's Records Management Policy currently being prepared, the Records Management Team will be liaising with Branches with a view to documenting and implementing a retention plan for all records, including those containing personal data held by their branches, having regard to legal and regulatory requirements in place.

2.8: Give a copy of his/her Personal Data on request from the Data Subject and, where required and necessary, correct, block or erase the Data requested by the individual

2.8.1: Under Section 3 of the Data Protection Acts, an individual, who believes that the Department keeps Personal Data in relation to them, may request from the Department in writing:

- Confirmation whether such data is kept by the Department
- A description of such data and the purposes for which it is held

2.8.2: Under Section 4 of the Acts, the person is entitled to:

- A copy of the data
- A description of the purposes for which it is held
- A description of those to whom the data may be disclosed
- The source of the data unless this would be contrary to public interest.

2.8.3: Right of access has a number of exceptions

Sections 4 and 5 of the Acts provide that the right of access does not apply in a number of cases. These exceptions are listed in detail at **Section 4.**

3. Subject Access Requests

3.1 Dealing with a request for access to personal information (Subject Access Request)

A request for a copy of Personal Data under the Data Protection Acts is called a Subject Access Request (SAR). This request should be made in writing to the Department's Data Protection Officer:

Data Protection Officer
Facilities Management
Department of Defence
Station Road
Newbridge
Co. Kildare

The request may be in the form of a letter from the Data Subject or alternatively, can be submitted on the Subject Access Request form - **see Appendix III**. The request must be accompanied by a copy of a current identification document (e.g. passport or driving license).

Unlike an FOI Request, a SAR does not have to stipulate that the request is being made under the Data Protection Acts. Where a written request for copies of personal information is received, it should be treated as if it was made under the Acts.

To facilitate processing of the SAR the individual should, where possible, give any details which might be needed to help the Department identify the individual and locate the information which it may keep about him/her (e.g. relevant section of the Department with which the individual has had interaction, previous address etc.).

3.2 Processing a Request

- An access request for a copy of all such Personal Data should be acknowledged as soon as possible and issued by the Data Protection Officer. **See Appendix IV.**
- A fee of not more than €6.35 may be requested by the Data Controller.
- Once the appropriate fee (if required) is remitted, contact will be made with the relevant Head of Branch requesting that a search be carried out for personal data which refers to the data subject.

- The retrieved data, including a schedule of the documents relevant to the request is submitted by the Head of Branch to the Department's Data Controller, who will consider the release of the information in accordance with the Data Protection Acts. If the Head of Branch recommends that some of the material should not be released, the schedule should refer to the sections of the Data Protection Acts 1988 and 2003 which apply in these instances.

- The reply should issue to the Data Subject within **40 days of receipt of the request.**

  When responding to an individual's request for access to personal data, they should be advised by the Department of their right to raise the matter with the Data Protection Commissioner and that they can do this by contacting the Data Commissioner on www.dataprotection.ie

If you are unsure how to deal with a particular query or have concerns about releasing particular types of personal information then contact the Department's Data Protection Officer, John Thornton on ext 2458.

4. Exceptions to provisions of the Data Protection Acts

4.1 Individuals have a strong right of access to see their personal data. However, Section 5 of the Data Protection Acts provides that individuals do not have a right to see information relating to them where any of the following circumstances apply:

4.1.1 If the information is kept for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, or assessing / collecting any taxes or duties: but only in cases where allowing the right of access would be likely to impede any such activities

4.1.2 If the information is kept for certain anti-fraud functions, and where allowing the right of access would be likely to impede any such functions

4.1.3 If granting the right of access would be likely to harm the international relations of the State

4.1.4 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

4.1.5 If the information would be subject to legal professional privilege in court

4.1.6 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

4.1.7 If the information is back-up data. It would be unreasonable to expect an organisation to retrieve back-up copies of its personal information in responding to an access request. However, it should be noted that back-up data is not necessarily the same as old or archived data. Such archive data is subject to an individual's right of access in the normal way. For more information on back-up data **see Appendix I.**

4.2 Restrictions on access to medical data and social work data.

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 an access request, if that would be likely to cause serious harm to the physical or mental health of the data subject. A person who is not a health professional should not disclose health data to an individual without first consulting the individual's own doctor or some other suitably qualified health professional.

Similar provisions apply in respect of social work data. The Data Protection (Access Modification) (Social Work) Regulations, 1989 (S.I. No. 83 of 1989) provide that social work data relating to an individual should not be made available to the individual in response to an access request, if that would be likely to cause serious harm to the physical or mental health or emotional condition of the data subject. The regulations apply to social work carried on by Ministers, local authorities, health boards, or any voluntary or other body that receives public funding for this work.

4.3 Information about Other Individuals

Section 4(4) of the Data Protection Acts makes special provision for dealing with the personal data of another individual. A data controller is not obliged to comply with an access request if that would result in disclosing data about another individual, unless that other individual has consented to the disclosure. However, the data controller is obliged to disclose so much of the information as can be supplied without identifying the other individual, e.g. by omitting names or other identifying particulars.

4.4 Expressions of Opinion

Where personal data consists of an expression of opinion about the data subject by another person, the data subject has a right to access that opinion except if that opinion was given in confidence. If the opinion was not given in confidence then the possible identification of the individual who gave it does not exempt it from access.

4.5 Examinations Data

Section 4(6) of the Data Protection Act makes special provision for responding to an access request about the results of an examination. "Examination" in this context means any test of knowledge, skill, ability etc., and is therefore not confined to official State examinations. Medical examinations are not however covered under these provisions. The special provisions under Section 4(6) allow

- for an increase in the time limit for responding to an access request from 40 days to 60 days, and
- deem an access request to be made at the date of the first publication of the examination results or at the date of the request, whichever is the later.

4.6 Disproportionate effort

Section 4(9) provides that the obligation on a data controller to comply with an access request applies unless it is impossible for the data controller to supply the data or it would involve disproportionate effort. If files are archived and are not used for decision–making as part of the day to day operations of the organisation, and retrieval involves disproportionate effort (or perhaps even cost where a storage company is used), then the data could be said to be not readily accessible.

In such a circumstance, the data subject would need to be able to identify particular data by file reference or date so that on a reasonable view of things the data could be said to be readily accessible. This restriction on the right to access should have narrow application in practice, the Data Protection Acts require that the right to access be guaranteed and would not appear to allow for this right to be refused outright because it results in a data controller exerting "disproportionate effort"

4.7 Repeated Access Requests

If a data controller has complied with an access request he does not have to comply with an identical or similar request unless a reasonable interval has elapsed.

5. Audits

As part of the process in developing a Data Protection Policy for the Department, the Data Protection Team has undertaken an audit of all personal and personal sensitive data held in each Branch. As a follow-up exercise, information has also been sought to determine if the current security measures are deemed adequate to ensure that the all such data is kept safe and secure. The Data Protection Team will use this information to compile an annual checklist which all Heads of Branches will be required to complete, as part of a yearly review, of data protection measures in their respective areas.

The Data Protection Commissioner has the right to carry out an audit on Department's data protection measures and advise on additional protection measures if deemed necessary.

6. Data Security Breaches

6.1 Types of Data Security Breaches

A data security breach can occur due to a number of reasons including the following:

- Loss or theft of data or equipment on which data is stored (including a break-in)
- Inappropriate access controls
- Equipment failure including security or IT equipment
- Human error
- Unforeseen circumstances such as a fire or flood
- Hacking offence
- Unlawful access to data

6.2 Guidance

The Data Protection Commissioner has published a **Data Security Breach Code of Practice** to assist organisations in the event of a Data Breach. In addition, the Department of Finance also provides guidelines on the proper handling of such breaches.

6.2.1 Notification of Breaches to Data Controller

All incidents of loss of control of personal data in manual or electronic form must be reported immediately to the Data Controller and the Data Protection Officer by the Head of Branch as soon as s/he becomes aware of the incident.

6.2.2 Risk Assessment

The Department of Finance guidelines recommend that in assessing the risk arising from a data security breach, the relevant Head of Branch should consider the potential adverse consequences for individuals, i.e. how likely it is that adverse consequences will materialise and, in the event of them materialising, how serious or substantial are they likely to be. In assessing the risk, Departments should consider the following points:

- what type of data is involved?

- how sensitive is the data?
- are there any protections in place (e.g. encryption)?
- what could the data tell a third party about the individual?
- how many individuals' personal data is affected by the breach?

6.2.3 Notification of Breaches to Data Subjects Affected

The Data Security Breach Code of Practice specifies that 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. Such information permits Data Subjects to consider the consequences for each of them individually and to take appropriate measures. In certain 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, or financial institutions etc.

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.

6.2.4 Notification of Breaches to the Data Protection Commissioner

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.

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.

Data Controllers reporting to the Office of the Data Protection Commissioner are requested to 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 through 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.

6.2.5 Report of the Data Security Breach

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.

6.2.6 Follow-up Investigation by the Data Protection Commissioner

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. Even where there is no notification from 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.

6.2.7 Internal Review and Evaluation

Subsequent to any Data Security Breach, the Department of Finance Guidelines recommend that a thorough review of the incident, by the Data Controller, the relevant Head of Branch and Data Protection Team, should occur.

The purpose of this review is to ensure that the steps taken by staff in the Department during the incident were appropriate and to identify areas that may need to be improved. Any recommended changes to policies and/or procedures should be documented and implemented as soon as possible thereafter.

Further information and guidance on the proper handling of Data Security Breaches are available in the **Data Protection Commissioner's Data Security Breach Code of Practice** and **the Department of Finance Breach Management Guidelines, CMOD, 2008, both on www.dataprotection.ie**

The Data Protection Policy is now also available on the Department DNET under 'Data Protection'.

APPENDICES

I. **Key Terms and Definitions in the Data Protection Field.**

II. **Personnel in the Department with a designated responsibility for Data Protection.**

III. **Subject Access Request Form (SAR).**

IV. **Sample Acknowledgement letter of receipt of Subject Access Request.**

V. **Submission to Data Controller.**

VI. **Acknowledgement.**

APPENDIX I

Key Terms and Definitions in the Data Protection Field

Data

Data is information in a form that can be processed. It includes automated, 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).

Personal data

Section 1 of Data Protection Act provides the following definition:

'Personal Data relates 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

Under the provisions of the Data Protection Acts, sensitive personal data refers to specific Personal Data such as:

- ***Racial or ethnic origin, political opinions, religious or philosophical beliefs***
- ***Whether the data subject is a member of a trade union or DF representative association***
- ***The physical, mental health or condition or sexual life of the data subject***
- ***The commission or alleged commission of any offence by the data subject. Any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any Court in such proceedings.***

Data Covered by the 1998 and 2003 Acts

The provisions of the Acts apply to any personal data that is obtained and processed by the Department, whether it is stored on lap-tops, paper, IT system, CCTV or mobile data devices.

Data concerning HR-related matters such as sick leave, performance, disciplinary, interviews etc. would be examples of data covered by the Acts.

Identifiable information concerns data which identifies an individual, eg occupation, address, physical characteristics etc.

Back-up Data

Back-up Data is defined in the Data Protection Acts, 1988 & 2003 as being ***" data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged".***

In order to come within the definition of 'back-up data', data cannot be part of a live system nor can it be used for any purpose other than replacing lost, destroyed or damaged data.

- ***Lost, destroyed or damaged Data***
  Data that is either accidentally, or deliberately, deleted can be considered to be destroyed. Data that can no longer be found may be considered to be lost. Damaged data may result from files being corrupted.

- ***The purpose of backing-up Data***

  There is a requirement in the Data Protection Acts that adequate measures be taken to prevent the un-authorised destruction or alteration of data

  2(1)(d) states that "appropriate security measures shall be taken against unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data.."

  By backing-up data, a Data Controller/Processor is taking steps to recover from such actions. In general, back-ups are most useful in a disaster recovery situation, where there has been a catastrophic system failure resulting in a large scale, if not total loss, or corruption of data.

- ***Retaining Back-Up Data***

  This will largely depend on how long after an event, that it is likely to be discovered that data has been lost, destroyed or damaged.

Data Subject

The Data Subject is the person who can be identified by the data held.

Data Controller

The Data Controller controls the content and use of personal data. For registration purposes with the Data Protection Commissioner's Office, **the Data Controller for the Department is Assistant Secretary, Des Dowling.**

Data Processor

The Data Processor is someone, aside from employees of the Data Controller, whose business consists wholly or partly in processing personal data. This includes external third parties under contract to the Data Controller.

The Data Protection Commissioner

The Data Protection Commissioner is Mr. Billy Hawkes, who is responsible for ensuring that peoples' rights under Data Protection legislation are respected and that the persons who keep personal information on computer or in manual format meet their responsibilities.

Privacy Audit

A Privacy Audit is an audit carried out by the Office of the Data Protection Commissioner of an organisation's data protection policies and procedures. The Data Controller gets advance notice of this audit and the primary aim of the '***Privacy Audit***' is to assist in improving data protection practices.

Information Notice

Under Section 12 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require any person or Data Controller to provide him with whatever information the Commissioner needs to carry out his functions, such as to pursue an investigation into a potential breach of data protection provisions. The Commissioner exercises this power by providing a written notice, called an ***'Information Notice'***, to the person.

Enforcement Notice

Under Section 10 of the Data Protection Acts, 1988 and 2003, the Data Protection Commissioner may require a Data Controller or Data Processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Data Protection Act, 1988 and 2003. Such steps could include correcting data, blocking data from use for certain purposes, supplementing data with a statement which the Commissioner approves, or erasing data altogether. The Commissioner exercises this power by providing a written notice, called an '***Enforcement Notice'***.

Data Security Breach

A Data Security Breach occurs when data, including personal data, has been lost or stolen through various means.

APPENDIX II

Personnel in the Department with a designated responsibility for Data Protection

Data Controller:

Des Dowling	Ext.	2130

Data Protection Officer:

John Thornton	Ext.	2458

Data Protection Team:

John Thornton	Ext.	2458
Maura Flanagan	Ext.	2123
Clair Gaffney	Ext.	2179
Carol Bourke	Ext.	2324

APPENDIX III

Subject Access Request Form

Application form for Data Access

Request for Data Access under the Data Protection Acts, 1988 and 2003.

Before completing this form, please read *Data Protection – Your rights from the Data Protection* Commissioner's website.

Answer all questions and indicate the appropriate details using an 'x' in the boxes provided.

Part One: Details of Data Subject

Contact Details

Full name:

Address:

Contact Number:

Email Address:

To assist in locating the personal information you require, please state the nature of the contacts you have had with this Department (eg letters, representations to Minister, previous submissions, emails etc):

Please provide any reference numbers relating to your contact with this Department:

Part Two: Details of Request

The Department of Defence has a number of data holdings within the Department. You can request personal information held under one or more of these data holdings by marking ‘x’ in the appropriate box or boxes below:

Data holding	**Tick as required**
Payroll, pensions, allowances	
HR, Attendance records	
Office Administration	
Lists of suppliers	
Contracts awarded	
Financial transactions with individual contactors	
Other	

Please outline below details of the data sought:

Part Three: Declaration

I declare that all the details I have provided in this form are true and complete to the best of my knowledge.

Signature of Applicant:_____ Date: _____

Please return the completed form to the **Data Protection Officer, Facilities Management, Department of Defence, Station Road, Newbridge, Co. Kildare.**

The Department is required to reply to the data subject within 40 days even if personal data is not held. For further information on Data Protection contact the Data Protection Commissioner's Office on tel: 1890 252231 or www.dataprotection.ie or email info@dataprotection.ie

APPENDIX IV

Sample Acknowledgement letter of receipt of Subject Access Request

Dear xxxxxxxxx,

I wish to acknowledge receipt of your correspondence dated xxxx in connection with your access request to personal data ……. held by this Department under the above Acts. I am satisfied as to your proof of identity.

Your request has been forwarded to the relevant Head of Branch within the Department who will communicate with you directly in this regard.

Under the terms of the Data Protection Acts, a reply must issue to you within 40 days of receipt of your request. This means that the data requested will be supplied to you by the xxxxxxxx

If I can be of any further assistance, in the meantime, please do not hesitate to contact me.

Yours sincerely,

_____

Data Protection Officer
Facilities Management
Department of Defence
Station Road
Newbridge
Co. Kildare

APPENDIX V

Submission to Data Controller

To Data Controller,

Attached please find request, under the Data Protection Acts, for access to all personal records relating to xxxxxx.

A decision on the request should be issued within 40 days of receipt of the request. This means that the data requested should be supplied to xxxxxx in the table below by xxxxxxxx.

The response to the requester is listed below and submitted for approval.

Schedule of Records – Summary of Decision Making

Record Number	Date of Record	Description of Record	Granted/Refused	Reason for refusal
1.				
2.				
3.				
4.				
5.				

In the response, the requester should be notified of the right of appeal if s/he is not satisfied and, if so, to contact the Office of the Data Protection Commissioner who have the authority to conduct a complete independent investigation of the matter.

Submitted please,

Principal Officer

Date:-

APPENDIX VI

Acknowledgement

All staff in the Department of Defence, on reading this Policy Document, are required to complete this acknowledgement.

Depending on your location, the signed acknowledgement should be returned to one of the following:

Newbridge: Clair Gaffney, Data Protection Team, Facilities Management.

Renmore: Sheila Burns, HR Branch.

Roscrea: John Fitzpatrick, Civil Defence Admin

1, , confirm that I have read and understand the contents of this policy document and am fully aware of my obligations in implementing the provisions therein when obtaining, processing, retaining and disposing of personal data and sensitive personal data during the course of my work in the Department of Defence.

Signed

Date: