An Roinn Forbartha
Tuaithe agus Pobail
Department of Rural and
Community Development

Department of Rural and Community Development Data Protection Policy & Procedures

---

May 2018

Table of Contents

Policy

An Roinn Forbartha Tuaithe agus Pobail
Department of Rural and Community Development

Remember that in relation to Data Protection and related data breaches, prevention is the best remedy. It is the responsibility of each member of staff of this Department to exercise utmost caution with regard to information and data held by the Department of Rural and Community Development.

This policy has been approved by the Management Board of the Department of Rural and Community Development and it describes the Department's procedures in relation to Acts and Legislation pertaining to the General Data Protection Regulation 2018.

1. Introductory Statement

What is Data Protection?
It is the safeguarding of the privacy rights of individuals in relation to the processing of their personal data. You supply information about yourself to government bodies, banks, insurance companies, medical professionals and many others in order to avail of services or satisfy obligations. Organisations or individuals also obtain information about you from other sources. For the purpose of data protection such organisations or individuals who control the contents and use of personal data are known as data controllers. The Data Protection Acts 1988 and 2003 give you rights relating to this personal information and impose obligations on data controllers. These rights apply where the information is held:
- on computer, or
- in a manual form, as part of a filing system that facilitates ready access to a specific individual's information.
These rights, which are outlined in detail in the remainder of this booklet, empower you to ensure that your information is accurate, is only made available to those that should have it and is only used for specified purposes. You may have to take action to enforce these rights by contacting the data controller concerned and if you have any difficulty enforcing your rights you can avail of the assistance of the Data Protection Commissioner

1.1 This policy specifies how Data Protection within the Department of Rural and Community Development is undertaken. It outlines the scope and purpose of the Department in relation to data collection and use, and the Data Protection principles the Department adheres to. It provides links and references to a number of other policies and procedures as they relate to data processing and control. It also contains the code of practice to be followed if a Data Breach occurs in the Department of Rural and Community Development. It also advises on the General Data Protection Regulations (GDPR) and its effects on this Department and the relationships and responsibilities of staff in relation to the GDPR.

1.2 The Department is committed to protecting the rights and privacy of individuals and Corporate services are fully committed to be compliant with all Data Protection legislation including that of the General Data Protection Regulation (GDPR) and in line with accepted good industry practices. The Data Protection Acts apply equally to personal data held on ICT systems and on paper files.

1.3 The Policy also sets out a number of related documents in the appendices including:

- Other policies impacting on Data Protection Policy
- DRCD Protection of Personal Data: Data Breach Management Plan
- Data Protocol for Service Management Agreement
- DRCD Information and Communications Technology Usage Policy
- DRCD and getting ready for the GDPR

2. Scope and Definitions

The policy applies to the keeping and processing of personal data, both manual and in electronic form, including personal data held on computer. It provides guidelines on how personal data is to be stored, handled and protected. This document should be brought to the attention of all staff but specifically to those whose work involves the handling of personal data.

Data: *means information in a form that can be processed. It includes automated data (information on computer or information recorded with the intention of putting it on computer) and manual data (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).*

3. Goals/Objectives

The policy intends to achieve:

- Full compliance with Data Protection Acts
- Compliance with the 8 rules of Data Protection laid out by the Data Protection Commissioner
- Safeguarding data of staff of the Department, suppliers and any internal or external stakeholder
- Awareness of and implementation of all aspects of the General Data Protection Regulation (GDPR)

4. Compliance with the Law

4.1 The Data Protection Officer (DPO) and Data Controllers ensure compliance with the law by being aware of relevant data protection responsibilities, in particular, to process personal data fairly. Staff must be made aware of their responsibilities through appropriate induction training with refresher training as necessary and the availability of an internal data protection policy that is relevant to the personal data held by the Department. This Data Protection Policy which reflects the eight fundamental data protection rules and are applied in the Department and is enforced through supervision and regular review and audit, is a valuable compliance tool. The Data Protection Acts are enforced by the Data Protection Commission whose role is to ensure that those who keep personal data comply with the provisions of the Acts. The Commission has a wide range of enforcement powers to assist it in ensuring that the principles of data protection are being observed. These powers include the serving of legal notices compelling data controllers to provide information needed to assist its' enquiries, and compelling a data controller to implement one or more provisions of the Acts in a particular prescribed manner.

The Commission may investigate complaints made by the general public or carry out investigations proactively. It 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. The Department and our staff are required to co-operate fully with such officers.

The Commissioner also publishes an annual report which names, in certain cases, those data controllers that were the subject of investigation or action by his Office.

A data controller found guilty of an offence under the Acts can be fined amounts up to €20 million, or 4% annual global turnover – whichever is higher, and upon conviction may be ordered to delete all or part of the database.

The Department of Rural and Community Development is committed to be proactive and fully compliant with the implementation of the General Data Protection Regulations (GDPR).

Under the General Data Protection Regulations (GDPR) the Office of the Data Protection Commissioner will become the Data Protection Commission.

5. General Procedures

5.1 - The first stage in establishing data protection policy and procedures to ensure the protection of personal data is to know what data is held, where it is held and what the consequences would be should that data be lost or stolen. With this in mind, the Department of Rural and Community Development is conducting an audit identifying the types of personal data held within the Department, identifying and listing all information repositories holding personal data and their location. Risks associated with the storage, handling and protection of this data will be included in the Department's risk register. The Departments can then establish whether the security measures in place are appropriate and proportionate to the data being held while also taking on board the guidelines available in this document. All risks cannot be eliminated, however potential risks will be identified and actions taken to minimise impacts should they occur. Please see the "Risk Management Policy of the Department of Rural and Community Development (DRCD)".

5.2 - Access to systems which are no longer in active use and which contain personal data should be removed where such access is no longer necessary or cannot be justified.

5.3 – The OGCIO provides ICT services to the Department and staff are obliged to sign and adhere to the policies that govern the supplied hardware and software.

- Each user of the Department of Rural and Community Development is allocated a username and password for their PC. The owner of a particular username is held responsible for actions taken under that username. All passwords are set to change on a regular basis.
    - Passwords must be kept secure and not disclosed.
    - Passwords must be at least ten characters in length, contain at least one upper and lowercase letter and include numbers.
    - Passwords based on repetition, dictionary words, letter or number sequences, usernames, or biographical information like names or dates must be avoided.
    - Passwords used to access PCs, applications, databases, etc. should be of sufficient strength to deter password cracking or guessing attacks.
- The Department can monitor stored files, email messages and internet access for auditing, investigative or security reasons.

- Users are only permitted to access electronic information and data that they require to perform their duties.
- PCs and notebook computers must not be left unattended for long periods while logged in e.g. during lunch, coffee breaks etc. Users must either logoff, set their computer to sleep or activate a password-controlled screensaver if they are leaving their PC.
- Confidential data held on computer media (e.g. external hard drive, flash drive) must be stored securely when not in use.
- Physical access to the servers will be restricted to staff authorised by OGCIO ICT Unit.
- Downloading of executable files or software within the Department of Rural and Community Development is strictly prohibited unless written authorisation is received from the OGCIO ICT Unit.
- OGCIO shall be responsible for best practice in maintenance, upkeep and upgrading of the security infrastructure and outlining staff compliance procedures.

5.5 - The Department will have procedures in place to properly evaluate requests from other organisations for access to personal data in its possession. Such procedures will assist the Department in assessing whether the release of personal data is fully justifiable under the Data Protection Acts including the GDPR. The Department will also ensure that access by staff of personal data for analysis or research purposes is fully justifiable and proportionate and fully compliant with the GDPR. In the case of error or breach of data protocols, the Department will adhere to the Personal Data Security Breach Code of Practice laid out by the Data Protection Commissioner, available at http://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

5.6 - Personnel who retire, resign or transfer from the Department of the Rural and Community Development should be removed immediately from mailing lists and access control lists. Relevant changes should also occur when staff are transferred to other assignments internally. It is the responsibility of the Department to ensure that procedures are in place to support this, i.e. so that notification is provided to the relevant individual(s)/Unit in a timely fashion.

5.7 - Contractors, consultants and external service providers employed by The Department of Rural and Community Development should be subject to strict procedures with regard to accessing personal data by way of formal contract in line with the provisions of the Data Protection Acts and the GDPR. The terms of the contract and undertakings given should be subject to review and audit to ensure compliance.

5.8 - The Department of Rural and Community Development Audit Committee, when determining in consultation with the Secretary General of the Department the work programme of the Departments' Internal Audit Unit (IAU), should ensure that the programme contains adequate coverage by the Internal Audit Unit (IAU) of areas within the Department which are responsible for the storage, handling and protection of personal data. The particular focus of any review by the Internal Audit Unit (IAU) 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 data protection regulations. Risks associated with the storage, handling and protection of personal data

will be included in the Department's risk register and risk assessments should take place as part of a Department's risk strategy exercise. Staff in the Department where necessary will be required to carry out Data Protection Impact Assessments (DPIA) and where a Data Protection Impact Assessments (DPIA) indicates that the processing would result in a high risk and staff are unable to mitigate those risks by reasonable means, then staff will be required to consult the Data Protection Officer (DPO) to seek that officer's opinion as to whether the processing operation complies with the General Data Protection Regulation (GDPR). 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, soon to be become the Data Protection Commission.

5.9 - The Department of Rural and Community Development will put procedures in place in relation to disposal of files (both paper and electronic) containing personal data. Staff of the Department should be aware of their legal obligations as set out in the National Archives Act, 1986 and the associated National Archives Regulations, 1988. It should be noted that incoming and outgoing emails which are "of enduring interest" are archivable records under the Act. The OGCIO conducts the secure disposal of computer equipment, including storage media, as part of its role as ICT service provider to the Department.

5.10 - Quality Customer Service documentation/customer charters will detail how customers' data is held and how it will be used/not used. Website privacy statements should be regularly reviewed to take account of any enhancements, new practices or additional services which involve the collection and use of personal data, especially in relation to the GDPR. Other than information necessary to carry out their normal duties staff must not issue any information to third parties unless they have clear authorisation to do so. Staff should be aware of their responsibilities with regard to policies and procedures, particularly with regard to confidentiality.

5.11 - New staff in the Department of Rural and Community Development should be carefully coached and trained before being allowed to access confidential or personal files.

5.12 - Staff should ensure that callers to the office or other unauthorised persons are unable to view personal or sensitive information whether held on paper documents or information displayed on PC monitors, etc. PC's should be locked when staff are away from their desks for lengthy period of times. Where possible, staff should be advised against saving files to the local disk. Users should be instructed to only save files to their allocated network drive.

5.13 - Personal and sensitive information should be locked away when not in use or at end of day. Appropriate filing procedures (both paper and electronic) should be drawn up by each individual section and followed by all staff.

5.14 - The Department advises that all staff should be careful in their use of the Personal Public Service Number (PPSN) in systems, on forms and documentation. There is a strict statutory basis providing for the use of the PPSN. This allows organisations use the PPSN in support of a provision of a public service to a customer. The Department of Social Protection manages the issuance and use of PPS Numbers. A

register of organisations that use the PPSN has been prepared and published to promote transparency regarding the ongoing use and future development of the PPSN as a unique identifier for public services. The register is available at: http://www.welfare.ie/EN/Topics/PPSN/Pages/rou.aspx

5.15 - It should be noted that any databases or applications in use by the Department of Rural and Community Development which contain personal data must be registered with the Office of the Data Protection Commissioner.

5.16 - Paper records
The Data Protection Acts apply equally to personal data held on paper files. The following guidelines should be followed with regard to personal and sensitive data held on paper files:

- Paper records and files containing personal data should be handled in such a way as to restrict access only to those persons with business reasons to access them.

- This should entail the operation of a policy whereby paper files containing such data are locked away when not required.

- Consideration should also be given to logging access to paper files containing such data and information items.

- Personal and sensitive information held on paper must be kept hidden from callers to offices.

- Secure disposal of confidential waste should be in place and properly used. If third parties are employed to carry out such disposal, they must contractually agree to the Department's data protection procedures and ensure that the confidentiality of all personal data is protected. Such contracts should contain clauses similar to those outlined in the section on 'Data Transfers' below.

- When paper files are transferred within a Department, this usually entails hand delivery. However, it should be noted that, in many cases, internal post in the Department ultimately feeds into the general postal system (this is particularly true for Departments with disparate locations like the Department of Rural and Community Development). In these instances, senders must consider registered mail or guaranteed parcel post service where appropriate. Procedures must be in place for ensuring that the data is delivered only to the person to whom it is addressed, or another officer clearly acting on their behalf, and not any other staff member. Consideration should also be given to the security of manual files when in transit internally.

- Facsimile technology (fax machines) should not be used for transmitting documents containing personal data.

5.17 – ICT Data records
The OGCIO provides ICT services to the Department and they grant access to ICT files to staff as advised by the Department. All staff have given written agreement that they will comply with OGCIO ICT Policies.

6. Implementation Arrangements, Roles & Responsibilities

The Department of Rural and Community Development is the owner of this Data Protection Policy as specified below:

Data Controller: The Data Controller (DRCD) is the Policy owner and takes direction on the policy, as it relates to the Department. The responsibilities of the Data Controller include the evaluation of the effectiveness of the policy in consultation with key stakeholders.

Data controllers need to take certain actions to ensure the rights of data subjects:

- **Transparency** - In the first place, measures must be taken by data controllers to provide any information or any communication relating to the processing to these individuals in a concise, transparent, intelligible and easily accessible form, using the language that is clear and plain. For instance, it should be done when personal data are collected from data subjects or when the latter exercise their rights, such as the right of access. This requirement of transparent information and communication is especially important when children are data subjects.

- **Right of access and right to rectification** - Under the General Data Protection Regulation (GDPR) data subjects have the right to obtain from data controllers a confirmation regarding the fact whether or not personal data in relation to them are being processed and to access these data. This is the so-called right of access found in Article 15 GDPR.

- **Right to object and right to restriction of processing** - Data subjects have the right to object under Article 21 GDPR. Exercising this right prevents the controllers from the further processing of personal data if there are no compelling legitimate grounds for continuing it.

- **Right to erasure and right to data portability** - The right to erasure (also known as “the right to be forgotten”) is to be found in Article 17 GDPR. It allows data subjects to obtain from data controllers the erasure of personal data concerning them without undue delay. This right, however, does not apply when, for example, the processing is necessary for the exercise of the right to freedom of expression and information; when there are reasons of public interest in the area of public health; or when legal claims must be established, exercised or defended. Data subjects also have the right to data portability or, in other words, the right to receive from controllers personal data concerning them in a structured, commonly used and machine-readable format and to transmit these data to other controllers. This has been laid down in Article 20 GDPR. If it is technically possible, personal data can be directly transmitted from one controller to another. The right to data portability is not applicable to the tasks

carried out in the public interest or in the exercise of official authority by the controller and it cannot be invoked to adversely affect the rights and freedoms of others.

- **The right to be forgotten** - Under Article 17 of the GDPR, data subjects have an important right to erasure, which is sometimes referred to as "the right to be forgotten".

- **Rights concerning complaints and judicial remedies** - Under Article 77 GDPR, data subjects have the right to lodge a complaint with a supervisory authority in the Member States where they live and work and places of alleged infringements if they think that the processing of their personal data infringes the GDPR. It means that if our personal data are processed by a person or entity in a way that is incompatible with the regulation, a complaint can be lodged about this with a supervisory authority.

- **Rights regarding automated decision-making, representation and compensation** - Article 22 GDPR establishes the right not to be subjected to a decision that is based only on an automated processing, including profiling. This right is applicable when such a decision has legal consequences for an individual or in a similar manner significantly affects him or her. If a company automatically collects and processes personal data on the internet users, engages in profiling and some decisions creating legal effects with regard to them are taken, data subjects can exercise their right not to be subjected to such decision-making. This right is not applicable when an automated individual decision is needed for entering into a contract or performing a contract between the data subject and a data controller, is authorised by the EU or Member State law to which a controller is subjected and which provides certain safeguards or is based on the explicit consent of the data subject. These decisions may not be based on the special categories of personal data unless it is done with the consent of involved individuals or for reasons of substantial public interest. Also, measures must be introduced safeguarding data subjects' rights, freedoms and legitimate interests.

- **Acting on a data subjects behalf** - Using another right found in Article 80 GDPR, data subjects can allow not-for-profit bodies, organisations or associations to act on their behalf by lodging complaints, receiving compensation and exercising some rights with regard to complaints and judicial remedies. These entities can also have the right to act independently of a data subjects' mandate if the Member States provide for this possibility.

- **Material or Non Material Damage** - If individuals have suffered material or non-material damage as a result of an infringement of the GDPR they are entitled to the right to receive compensation from the controller or processor, as stressed in Article 82 GDPR. Controllers involved in the processing are liable for this damage; processors are only liable when they have not complied with their GDPR obligations or acted outside lawful instructions of controllers or contrary to them. Bodies, organisations and associations can also invoke this right on behalf of data subjects. The right to compensation can be exercised before competent courts of EU Member States

Data Processor: The Department of Rural and Community Development is a Data Processor.

Data Protection Officer: A Data Protection Officer (DPO) is appointed by the Secretary General as accounting officer of the Department in conjunction with both the Management Board and Corporate Services section. The responsibilities are to drive, support and oversee the implementation of the policy within the Department of Rural and Community Development to ensure all staff are fully trained, are aware of the policy and to receive notification of any updates or changes as required. The DPO is also responsible for working with the Incident Lead and reporting to the Data Controller when a breach occurs. The DPO will play a lead role and be proactive in implementing the contents of the General Data Protection Regulations (GDPR). The Data Protection Officer's role will also include a continual assessment as to whether the Department's current and future approach to data protection compliance will meet the GDPR's requirements

Incident Lead: An Incident Lead is an Assistant Principal in the Department of Rural and Community Development assigned at the time of a data breach to manage the data breach which has occurred in his/her business unit.

Note: Each Public Service Body (PSB) that the Department deals with is also a Data Controller and should therefore have their own stringent data protection policies in place.

7. Reviewing and Evaluating the Policy

Practical means will be used to ensure the impact and effectiveness of the policy. Examples include:

- All staff working in the Department of Rural and Community Development receive training in the 'Data Protection Legislation and Procedures' including that of the contents of the General Data Protection Regulations (GDPR) and are aware of the policy.

- The Data Protection Officer (DPO) conducts an audit for compliance with the policy.

- Requests for access to personal data are dealt with promptly and effectively.

- Personal data records are accurate.

- Personal data records are held securely.

- Personal data records are retained only for as long as necessary and within legal limits.

The Policy will be reviewed by the Data Protection Officer (DPO) in conjunction with the Corporate Office and the Management Board of the Department at the end of each

financial year; to ensure the Policy is fit for purpose and is aligned with any legislative changes. Changes required to the policy will be reviewed and approved by the Department's DPO, on behalf of the Department and approved by the Management Board.