The Irish Agriculture and Food Development Authority

Teagasc Personal Data Retention Policy			
Author	Ronan Coady	**Approved By**	ICT Committee
Valid From	08/11/2018	**Approval Process**	ICT Committee

1. Background

In response to the introduction of new EU and Irish legislation on the protection of personal data (GDPR and Data Protection Act 2018), Teagasc established a project team to review its compliance with data protection legislation. Teagasc had previously established a project to review its records management policy and processes. It is clear that there is a considerable overlap between Records and data assets containing personal data, but it is also clear that they are not the same thing and need to be considered differently. For that reason there are two different policies but a joint register of records and data assets containing personal data will be established and maintained by the Data Protection Officer.

2. Purpose of the Policy

The purpose of this policy is to define Teagasc's approach to the retention and destruction of Personal Data.

3. Applicability

The policy applies to all Teagasc staff, persons working on a contract basis for Teagasc, all students, fellowship holders, seconded staff and employees and agents of other organisations who directly or indirectly have access to Teagasc information assets (physical or electronic) or who process information on behalf of Teagasc, or its subsidiary Moorepark Technology Limited.

This policy is mandatory and by accessing any Teagasc information assets (physical or electronic) for which Teagasc is a Data Controller or Processor, users of Teagasc's information assets are agreeing to abide by the terms of this policy.

4. Policy Statement

Principles

1. In accordance with Data Protection law, personal data should be stored only for such period as is necessary in relation to the purpose for which the data are collected.
2. Personal data stored by Teagasc should be adequate, relevant and limited to what is necessary for the purpose for which it is processed.
3. All reasonable measures should be taken to ensure that personal data is accurate.

Ownership

4. All data, irrespective of format, generated, created, received and/or retained by those to which this policy applies is the property of Teagasc and subject to its overall control. Those leaving the organisation or changing positions within it are not to remove any data without the prior written authorisation of the Information Owner.

Storage

5. All personal data must be stored in a safe, secure and accessible manner to ensure the security and confidentiality of such data.
6. Special care is to be taken to ensure that special category personal data is stored in a secure manner which may include, for example, locked filing cabinets and offices for hard copy data and/or the use of password protection and encryption for data stored in electronic form.

Registration

7. The Data Protection Officer maintains a Data Protection Register which includes retention details for classes of information assets.
8. All personal data stored on behalf of Teagasc must be covered by an entry in the Data Protection Register.
9. It is the responsibility of each manager to ensure that the entries in the Data Protection Register cover all of the personal data being processed by their business unit.

Data Retention

10. Where the register contains minimum retention periods, data must be retained for the minimum period required.
11. A maximum retention period must be specified for all entries in the register.

End of Life

12. At the end of the retention period, Personal Data must be securely destroyed or anonymised within one year, subject to the following exceptions:
    a. Personal data may be further used for scientific research, subject to controls included in the data management plan for the research project in question
    b. Personal data must be retained where a *litigation hold* is in place in relation to the data
13. Destruction of physical special category personal data should be by shredding or use of a confidential waste disposal firm

End User Computing

14. Personal data should generally be stored only in Teagasc's ICT Application Systems or on shared drives which are subject to appropriate access controls. Personal data may be stored on a Teagasc desktop computer, encrypted laptop or encrypted portable storage medium (CD, USB stick, portable drive etc) for the completion of specific tasks. Every user who stores such data is responsible for:
    a. Ensuring that the data is registered in the Data Protection Register or covered by an existing entry in the Data Protection Register, and
    b. Reviewing such data on an annual basis and ensuring it conforms to its retention period in accordance with its data protection register entry.

5. Enforcement

Breaches of this policy may result in HR disciplinary procedures being invoked. Individuals should be aware that they as well as the organisation are individually liable to summary conviction under the Data Protection Acts if found guilty of knowingly or recklessly contravening its provisions. Breaches by individuals who are not staff will be dealt with by the appropriate line manager.

6. Definitions and Terms

Personal Data	means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an

	identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person[1]
Special Category Personal Data	are personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data[2]
Data Subject	is an individual who is the subject of personal data
Data Controller	means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Data Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Data Protection Register	refers to a set of records in relation to personal data, which is maintained by the Data Protection Officer and which may be published on the Teagasc public website. The register includes: • Information on systems and manual data sets (physical and electronic) which contain personal data • Information on personal data retention periods • Information on data protection impact assessments • Information on third parties with whom Teagasc exchanges personal data • Information on personal data flows into and out of Teagasc Due to the significant overlaps in the nature of records management and data protection requirements, a single register will be used to track information assets which may be used for one or both purposes.
Information Asset	is any artefact, in paper, electronic, or any other format, which is used to store information. An *information asset* may or may not contain *personal data* and may or may not be a *record*.
Information Owner	is the individual with primary responsibility for the data within an ICT System or a manual filing system. In the case of ICT systems. Information Owners are sometimes also referred to as the System or Project Sponsor.
Litigation Hold	is a notice from an authorised Officer of Teagasc that the destruction of data must stop immediately because of an on-going or potential litigation or an official investigation. Destruction may begin again once the Chief Operations Officer has confirmed that the relevant litigation hold has been lifted.
Record	is information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity. e.g. Minutes of Authority and Senior Management meetings. Approvals required as part of Government policy or by legislation

[1] Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, Article 4(1)
[2] Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, Article 9(1)

7. Related Documents

Links to related documents if applicable

8. Revision History

Revision date	Version	Summary of Changes
05/11/2018	0.1	Original
07/11/2018	0.2	Include comments from COO

Appendix A – Draft Content of Data Protection Register Entries for Personal Data

- Department
- Responsible Unit
- Responsible Person(s)
- Item Description
- Minimum Retention Period
- Maximum Retention Period
- Reason for Retention
- Type of Personal Data Held
- Does it include Special Category Data
- Is the item a Record
- Storage Location
- Access Controls