Department of Employment Affairs and Social Protection

February 2020

Data Retention Policy - Guidelines and Procedures

An Roinn Gnóthaí Fostaíochta agus Coimirce Sóisialaí
Department of Employment Affairs and Social Protection

Table of Contents

1. Executive Summary

This document sets out a corporate data retention policy for all data across all aspects of the Department's business. As such it is a living document, subject to ongoing review and update.

The Department's mission is "***To promote active participation and inclusion in society through the provision of income supports, employment services and other services"***

To undertake our mission, we need to collect personal data from our customers and from other sources as provided for by our legislation. The Department also collects personal data in relation to its staff and contractors.

In assuming responsibility for the personal data of our customers, in both paper and electronic form, this document sets out the policy for the retention of that data in the Department.

The policy recognises the scale and complexity of the Department's business and the associated scale and complexity of the data which the Department holds. It also recognises that there are complex data interlinkages within and between different operational scheme areas for identity authentication, assessment, award, maintenance, secondary payments and closure of data subject payments.

In drawing up this policy, a detailed examination of all of the Department's business areas was made, covering:

a. scheme administration,
b. policy formulation,
c. internal administration (HR/Accounts/control),
d. other social and employment areas managed by the Department, and
e. legislative requirements in these areas

This data retention policy takes account of:

- current legislative requirements concerning data retention;
- the requirements of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018;
- The requirement under the National Archives Act 1986; all records of Government Departments must be preserved and transferred to the National Archives when they are thirty years old, unless their disposal has been specifically authorised by the Director of the National Archives.

- the fact that customers of the Department can request a review of a Deciding Officer's or an Appeals Officer's decision at any time under Sections 301 and 317 or 318 of the Social Welfare Consolidation Act 2005, as amended; and

- The Department's responsibility to prevent, detect, investigate and prosecute cases of social welfare fraud. This will require the retention of scheme data and data collected for the purpose of identity authentication to be kept for the lifetime of the person plus 10 years.

The GDPR advises that "personal data shall be kept in a form which permits identification of subjects for no longer than is necessary for the purposes for which the personal data are processed;" (Article 5(1) (e)).

Due to the specific nature of data processing in the Department and its use for determining entitlements to payments and services over a person's lifetime, the Department distinguishes between data which should be retained for the lifetime of the person plus 10 years, and data which has been collected for a specific time-bound purpose, after which the data can be disposed of/erased.

Business areas also retain non-personal data such as policy, procedural, planning and general management documentation.

Any retention period proposed by a business area which is outside the retention periods below will require justification by the business area owner.

Business area example	**Retention Period**
Local project work of finite duration	Maximum of One Year
Scheme Areas	The lifetime of the person plus 10 years
Identity Authentication	The lifetime of the person plus 10 years
Other Business Areas	As decided by each Business Area and notified to the Data Protection Unit

2. Purpose

2.1 This document sets out a corporate data retention policy for data across all aspects of the Department's business. As such it is a living document, subject to ongoing review and update.

2.2 The purpose of this data retention policy is to provide advice and detail regarding the length of time that is appropriate to retain data processed by the Department or third party bodies/ agents acting on its behalf. The Department will only retain personal data for as long as it is necessary to do so and in accordance with all relevant laws and policies. The policy outlines the key considerations to which those responsible for data must have regard in determining how long various types of data may (or must) be retained; and when data may (and in some cases must) be destroyed.

3. Scope

3.1 This policy concerns all data processed by, or on behalf of, the Department (including data held on physical and/or electronic media). It includes, but is not confined to, personal data.

4. Definitions

(i) *Data deletion* - can mean different things in relation to electronic data, and we recognise it is not always possible to delete or erase all traces of the data. The key issue is to ensure data is put beyond use. If it is appropriate to delete personal data from a live system, consideration should also be given to the deletion of it from any back-up of the information on that system.

(ii) *Data retention* – for the purposes of this policy, data retention is the continued storage of the Department's data for compliance or business reasons. Under GDPR principles, personal data must be retained for no longer than is necessary

(iii) *Personal Data*: Any piece of data which, on its own, or with other data, can be used to identify a living individual (GDPR, Article 4[1]).

(iv) *Processing*: Any operation performed on data – the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

[1] 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural 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, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

(v) *Record*: Various different pieces of legislation provide a definition of a record or data, including the Freedom of Information Acts 1997 – 2014 and the Data Protection Act 2018.

For the purposes of this policy, a record is any item containing personal data, whether that item is printed (hard copy) or stored electronically. A record is also information in any format, created or received and maintained by the Department that provides recorded evidence of functions, activities and transactions in pursuance of legal obligations or in the transaction of business.

(vi) *Special Categories of Personal Data* in line with Article 9 of the GDPR: Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

(vii) *Trigger date for retention purposes*: The point from which the data retention period is deemed to begin. For the purposes of this policy, the retention period of a record of the Department is deemed to commence when the record is first created.

5. Background

5.1. Because of the nature and scope of its business, the Department holds considerable volumes of data, in both physical and electronic format, on customers, citizens and staff members. Customer data is required to ensure that entitlements are fairly and quickly processed. Different forms of aggregated customer-related data are also required by operational management, accounts, expenditure estimates and policy development. The Department also processes information relating to its own personnel for which civil service wide data retention policies apply.

5.2. The Department is subject to a wide variety of legal and regulatory requirements that prescribe minimum and maximum periods for the retention of the various types of data that it processes. The Department is committed to effective records management, retention and disposal to ensure that it:

- meets legal standards in terms of retention periods;
- optimises the use of space;
- minimises the cost of record retention; and
- securely destroys outdated records

6. Objectives

The objectives of this data retention policy include:

6.1. Ensuring that Departmental records are retained for as long as they have administrative or legal value.

Under the GDPR, organisations are not permitted to retain personal data for longer than is necessary. GDPR Article 5(e) emphasises that retention is "subject to the implementation of the appropriate technical and organisational measures required by the Regulation in order to safeguard the rights and freedoms of the data subject". Good housekeeping also dictates that we regularly review the need to retain records.

The GDPR does not dictate how long we should keep personal data. It is up to the Department to justify this, based on our purposes for processing. We are in the best position to judge how long we need data based on the retention periods being both necessary and proportionate to the purpose.

6.2. Ensuring that Departmental records are disposed of after minimum legal retention requirements have been met.

6.3. Avoiding the unnecessary retention of Departmental records that have no enduring archival or evidential value.

6.4. Ensuring that records worthy of permanent preservation are retained and are transferred to the National Archives at the appropriate time in line with agreed procedures.

6.5. Ensuring that Authorised Disposal Certificates are issued by the Director of the National Archives prior to the disposal of any records.

7. Benefits

The benefits that will derive from successful implementation of this data retention policy include:

7.1. Compliance with legislative and regulatory provisions regarding the retention of records, including the National Archives Act, 1986, the Data Protection Act, 2018 the GDPR and the Freedom of Information Act, 2014.

7.2. Avoidance of unnecessary accumulation of records in both paper and digital formats.

7.3. Controlled disposal of records in a managed and co-ordinated manner, in compliance with section 7 of the National Archives Act, 1986.

7.4. Financial savings with regard to the use of commercial storage companies for the unnecessary retention of records that do not warrant permanent preservation as archives.

7.5. Efficient identification of records of archival value.

8. Key Considerations about data retention

8.1. In all decisions about the retention of data, due regard must be had for the legal and regulatory requirements of retention for the type of data being processed. These include:

- General Data Protection Regulation (GDPR) considerations
- Data Protection Acts 1988, 2003 and 2018
- National Archives Act 1986
- Comptroller and Auditor General requirements
- Public Accounts Committee considerations
- Potential litigation/ appeal/ reviews requiring documentary evidence
- Internal Audit considerations

9. Proposed Data Retention Periods

9.1. The retention and disposal of records is determined by specific Social Welfare legislation, Employment Rights legislation, the National Archives Act 1986, the Data Protection Act 2018, (and the former Acts of 1988 and 2003) and the GDPR.

9.2 Under the National Archives Act 1986, all records of Government Departments must be preserved and transferred to the National Archives when they are thirty years old, unless their disposal has been specifically authorised by the Director of the National Archives.

The National Archives Office's role is to assist in preserving archival records by selecting those of permanent value, managing their transfer to the National Archives and facilitating the disposal of those records no longer required for administrative purposes or archival preservation.

9.3. Because of the range of data held, the various reasons why it is required, the different media on which it is stored, and the range of relevant legal requirements, the general data retention periods for the Department have been split into the following main categories:

Business area example	**Retention Period**
Local project work of finite duration	Maximum of One Year
Scheme Areas	The lifetime of the person plus 10 years
Identity Authentication	The lifetime of the person plus 10 years
Other Business Areas	As decided by each Business Area and notified to the Data Protection Unit

9.4. If business owners have data retention policies and practices which are of different duration to the above, these should be continued. Where relevant, each business area should also ensure that their documented retention policy and retention periods (if they

deviate from the policy and retention periods outlined in this document) are available, on request.

9.5. This data retention period for each work stream if different to the above should be documented at local level and **Appendix A** attached to this document completed and returned to the Data Protection Unit at MBX-DPO.

10. Retention of certain personal data for the lifetime of the person plus 10 years

10.1. Social insurance contribution records, PPSN, past claim data and identity data are retained for the lifetime of the person concerned plus 10 years. This is necessary and proportionate for the following reasons:

a. in order that a person can claim entitlement to services and benefits – many of which may not fall due until the occurrence of a particular event – the date of which cannot be known, e.g. illness, disability, caring responsibilities or widowhood.

b. due to payment and entitlement linkages between scheme areas during a customer's lifetime. Prior claim data is required as it can affect entitlement to future payments, because, under law, a person can request a review in respect of any claim decision at any time. Also, it can be necessary to inform an investigation into a prior fraud or error which is detected on the occasion of a subsequent claim or life event;

c. to enable deciding officers to carry out their statutory functions. Decisions relating to entitlement to social welfare payments and to insurability of employment are made by 'deciding officers' appointed by the Minister. Section 300 of the Social Welfare Consolidation Act 2005 (SWCA) provides that every question to which it applies, save when the context otherwise requires, shall be decided by a deciding officer. Deciding officers make all decisions concerning claims for and disqualification for all social insurance benefits and also decide all questions concerning entitlement to social assistance payments (except Supplementary Welfare Allowance) and child benefit (for a full list of all matters on which deciding officers make decisions please see section 300(2) of the SWCA). In order to carry out their statutory functions, deciding officers process relevant personal data of customers seeking decisions on their entitlements under the SWCA;

d. Section 301 of the SWCA 2005 grants a deciding officer a discretion to revise his or her decision or that of another deciding officer or a designated person, '**at any time'** in the following circumstances; in light of new evidence or of new facts; a mistake in relation to law or facts or; where there has been a relevant change in circumstances since the decision was given. An appeal can be made against a revised decision. In order for deciding officers to exercise the statutory functions in regard to revision of decisions and for customers to avail of the revision provision in Section 301, personal data must be retained by the Department;

e. current legislation allows that whilst there is a 21 day timeframe for making an appeal, the Chief Appeals Officer retains discretion to accept a late appeal if the circumstances warrant it.

Legislation, in effect, facilitates that virtually any Deciding Officer/Designated Person (DO/DP) decision can be revised at any future stage. Furthermore, customers of the Department can still request a review of an Appeals Officer's decision **at any time** under Section 317 or 318 of the Social Welfare Consolidation Act 2005. However, it is important to recognise that the use of "at any time" in Sections 317 and 318 mirrors the same wording in Section 301. Historically, the courts have not been inclined to support any narrowing of interpretation of that very broad scope of **"at any time"**.

A High Court Judgment by Justice Hogan, delivered on 14/11/13, arising from proceedings brought by a Department customer against the Chief Appeals Officer and the Minister reinforces this position[1]. The judgement in this case ruled that Section 317 of the 2005 SWCA Act "vests the Appeals Officer with a discretionary power of revision in circumstances which suggest that the decision may have been erroneous in the light of the emergence of new evidence, or new facts or where it appears that there has been a change of circumstances since the first decision was given." (Section 13 of this Judgement). The judgement held that the "express language of S.317 which provides that this revision may be done "at any time". This is very straightforward language which clearly provides that the power to re-open otherwise concluded appeals decision is not directly limited by temporal constraints" (Section 15 of the Judgement). The High Court Judgement also ruled that "Section 317 of the 2005 Act clearly confers such a jurisdiction to entertain revision applications of this nature in cases where new evidence has been presented" (Section 24 of the Judgement).

For these reasons, the Department is obliged to retain scheme data for the lifetime of the person plus 10 years.

f. PPSN and identity data is critical to the prevention, detection and prosecution of identity fraud, which again can occur at an unknown time. It is also critical to the efficient administration of estate cases (i.e. payments made or refunded after a person dies). Estate cases can take a number of years to resolve.

[1] High Court record number 2014 607 JR refers – CP Vs Chief Appeals Officer and others 14/11/13 – Citation number [2013]IEHC 512

All original documentation, including photographic images, underpinning SAFE 2 registration is required to enable any future prosecution for fraud or other criminal activity.

The Department has a key role in ensuring that public monies are paid to the correct person and requires that where criminal activity, such as identity fraud or benefit fraud is detected, it is necessary that evidence can be adduced to successfully institute a prosecution in conjunction with the Director of Public Prosecutions or Chief State Solicitor's Office. The original documentation or retained certified copies are central to proving the constituent elements of a fraud, involving identity. Accordingly, the documents are necessary to carry out that prosecutorial function.

Evidence has to be adduced establishing and proving the process of identity authentication and the documentation underpinning same. In such instances, the production of original evidence of address, for example, can provide the key link between two identities that are at issue. Given the nature of criminal activity such as fraud, such fraudulent activity could occur weeks or years after the original assessment. Therefore, it is necessary to keep such documentation for the lifetime of the person plus 10 years.

10.2 Documents that support claim and identity data (e.g. documents evidencing income and identity) may be retained for so long as the claim and identity data is retained. This is necessary in order to support prosecution and resolution of any issue that may emerge relating to a person's entitlement to a service or benefit or to their identity. For example, even after a claim closes or a service ceases, issues can arise when a person's estate is being settled, when the person subsequently claims another benefit or service or when another person seeks to claim a service or benefit in the name of the first person. In addition, the Department can be called upon at any time to verify the identity of any person to whom it has issued a PPSN.

10.3 Where data (other than social insurance contribution, PPSN, identity, and claim data) is collected or processed as part of an ongoing department/client relationship then it may be retained for the lifetime of that relationship plus ten years. (For example data relating to the provision of employment services to a person will be retained for so long as the person concerned is in receipt of employment services plus up to ten years). The retention of the data for up to a ten year period after the direct service relationship ends enables the Department to access prior service history in the event that the person concerned re-engages with the service at a future date.

10.4 Where other transactional data is collected it will be deleted as soon as its purpose has been served. An example of this is where the Department may generate customer lists for invitations to jobs fairs. These lists will be deleted once the event that they were prepared for has concluded.

10.5. Any proposal on whether to retain personal data for a specified period outside the options listed above would require decision by the relevant business area owner.

11. Disposal / Destruction of Data

11.1. Once the retention period has been identified, it should also be noted that no class of Departmental records can be destroyed without first obtaining a disposal certificate from the Director of the National Archives of Ireland.

11.2. A record may not be destroyed if any litigation, claim, negotiation, audit, open records request, administrative review, or other action involving the record is initiated before the expiration of the retention period.

11.3. Data retention policies specific to business areas (if different to this policy) and data retention periods should be documented locally and held in a format that they can be examined and inspected by the supervisory authority – the Data Protection Commission in the case of personal data.

11.4. Arrangements for the deletion of electronic records in line with the business area's data retention policy will have to be agreed and co-ordinated with IS Division and then documented locally and copied to the Department's Data Protection Officer at MBX-DPO.

11.5. Any destruction/disposal of records will be carried out on a phased basis due to the complexity and volume of data.

11.6. A certain percentage of the Department's records are worthy of permanent retention owing to their historical and evidential value as archives. These records will normally relate to functions, structures and activities of the Department. Under the National Archives Act 1986, all Department records which are retained permanently should be transferred to the National Archives of Ireland when they reach 30 years old unless they qualify for retention under Section 8(4) of the National Archives Act, in which case, retention authorisation must be obtained from the National Archives of Ireland.

11.7. From a records management and archival point of view, the retention of much of the material produced by the Department as part of the administration of payment schemes has no archival value and will not be subject to the derogations under article 89 and article 5, GDPR for retention beyond its business use.

12. Compliance

12.1 Due to the volume and complexity of records, the implementation of this policy will be carried out on a phased basis by relevant business managers, in conjunction with Facilities Management Unit and ISD.

13. Data Ownership

13.1. Data and information assets will have a clearly identified owner which will generally be vested in each business area. These data owners will be responsible for ensuring compliance with this policy in respect of the data and information assets for which they are responsible.

14. Third Party Contracts

14.1. Where data is processed by a third party body/ agency acting on behalf of the Department, a contract or agreement must exist between the business area responsible for acquiring that service and that third party organisation.

14.2. Where appropriate, third-party contracts must include details of the retention policy for the data provided and the disposal requirements once the retention time-limit has been reached. It is the responsibility of the data owner to ensure that the contractor is aware of the data retention time limits on the data.

14.3. The Data Protection Unit can assist in general guidance and assistance in respect of data transfers and third party contracts where personal data is processed.

15. Review

This data retention policy will be reviewed periodically by the Department and will be amended and updated, as appropriate, following approval by the Data Management Programme Board. Any updates will be published on the Department's website.

Appendix A

Document Retention Record

To be completed and returned, to the Department's Data Protection Unit – DPO@welfare.ie
Where business areas have retention periods other than those set out in this policy, (due to legislative requirements for instance) these should be outlined using the template below.

Section	Document Description	Paper/Electronic	Period of retention

Appendix B

Additional Resources

Legislation

National Archives Act, 1986: http://www.irishstatutebook.ie/eli/1986/act/11/enacted/en/html

National Archives Act, 1986, Regulations, 1988:
http://www.irishstatutebook.ie/eli/1988/si/385/made/en/print

Data Protection Act, 2018: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR):
https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=celex:32016R0679

Websites (National)

National Archives: www.nationalarchives.ie

National Archives guidance note on compatibility with GDPR:
http://www.nationalarchives.ie/wpcontent/uploads/2018/05/20180319GDPRNAA_GuidanceNote_3.pdf

Data Protection Commission: www.dataprotection.ie, www.gdprandyou.ie

Websites (European)

Article 29 Working Party: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358