



ÚDARÁS UCHTÁLA na hÉIREANN
THE ADOPTION AUTHORITY of IRELAND

Retention & Disposal Policy

Revision and Approval History					
Version	Revised By	Revision Date	Approved By	Approval Date	Comments
Draft	DPO	04/4/2019			
Draft	Head of Compliance & Resources/DPO	04/04/19			
Reviewed	DPO	13/07/2020			
Reviewed	Mathesons	18/10/2020			
Reviewed	DPO	26/01/2021			
Reviewed	DPO	1/4/2021			

Reviewed	Board	13th April 2021			
-----------------	--------------	---------------------------------------	--	--	--

Contents

1	Introduction	3
	Policy Scope	3
	Exceptions to this Regulatory Requirement.....	3
2	Defining data retention requirements.....	4
	High level regulatory requirements.....	4
	Considerations when defining retention periods.....	4
	Legal and regulatory vs the Adoption Authority defined retention periods.....	5
	Default personal data retention periods.....	6
3	Recording and reviewing retention requirements	7
	Notifying data subjects and internal record keeping	7
	Review of Retention	7
4	Taking action when the retention limit is reached.....	8
	Processor retention requirements	8
	Managing retention policy exceptions	8
5	Disposal of Records	9
	Review of Disposal.....	9

1 Introduction

The General Data Protection Regulation (GDPR) requires the Adoption Authority of Ireland (the “**Adoption Authority**”) to only retain personal data while there is a valid legal reason to do so. Data subjects will be informed about the planned period of retention when data is collected to enable them to make an informed choice about sharing their data. Over-retention of data increases the risk that data will become inaccurate, lost, stolen, disclosed, shared too widely, and/or used inappropriately.

This poses a growing risk to the rights and freedoms of data subjects and to the Adoption Authority. In addition, while personal data is retained, the data controller and any processors handling that data must secure the data and respond to any request from a Data Subject to exercise rights specified in GDPR Articles 12 to 22.

GDPR Article 5(1)(e), the storage limitation principle, outlines retention requirements and is one of the 6 core principles in the GDPR that are reflected in the detail and interpretation of all relevant parts of the regulation.

A number of terms used in this policy are outlined in greater detail in the ***Glossary of Data Protection Terms***.

Policy Scope

This policy sets out the Adoption Authority’s responsibilities to comply with GDPR Article 5(1) e: the storage limitation principle and related requirements in Article 13: a data subject’s right to be informed about details of planned processing when data is collected.

This policy should be read and used in conjunction with the Adoption Authority’s Policy on Lawful Personal Data Processing. In addition, you should refer to any pre-existing records management, information governance, or information rights management policies.

We have sought legal advice on the status of some data currently held in the Adoption Authority, and are awaiting legal definitions in legislation to establish the status of this data. Until such clarifications are received our policy will be to retain this data in perpetuity.

Exceptions to this Regulatory Requirement

Where we have a verifiable legal responsibility to indefinitely retain any subset of personal data, the storage limitation requirements in this policy will not apply to that data. This does not absolve us of responsibility to comply with applicable GDPR security, accountability, data management, and data subject rights management requirements.

If personal data is rendered anonymous so that it cannot be used to identify any living individual, either by using the data set, or supplementary data readily available, then requirements in this policy do not apply.

2 Defining data retention requirements

High level regulatory requirements

Article 5(1)(e) states that personal data shall be:

“...kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')”.

Considerations when defining retention periods

The legal basis for collecting and processing data and associated retention requirements will be defined before data is collected. Information which will be gathered before processing data includes:

1. The purpose(s) for collection. This could, for example, be to provide a service or to enable research or to prepare a contract.
2. The type and quantity of data to be processed for each defined purpose. In particular identifying subsets of;
 - a. Special category data
 - b. Data relating to children
 - c. Convictions data
3. The minimum quantity of personal data and the minimum amount of personal data fields and or data types required to serve the defined organisational purpose, crucially asking:
 - a. Can personal data collection and processing be reduced to reduce risk to the data subject and comply with the data minimisation principle (Article 5(1) (c)?
 - b. Can the purpose be served using anonymised data? If yes, this removes the requirement to limit storage and places the data set out of the scope for other GDPR control.
 - c. If it is essential to use personally identifiable data for this purpose, will that change in future? Switching to use of anonymised data removes any applicable storage limitation requirement, and if the retention limit has been reached, it is an alternative to data deletion.
4. The legal basis for processing personal data for each defined purpose is :

- a. **Consent** – Processing on the basis of unambiguous, informed, and freely given consent from the data subject for the specified purposes.
- b. **Contract** - Processing necessary for performance of a contract.
- c. **Legal** - Processing necessary for compliance with a legal obligation to which the controller is subject.
- d. **Vital Interest** - Processing necessary in order to protect the vital interests of the data subject or of another natural person.
- e. **Public Interest** - Processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. This is the basis primarily relied on in the Adoption Authority.
- f. **Legitimate Interest** - Processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party (for example for information security purposes, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.)

Legal and regulatory vs the Adoption Authority defined retention periods

The Adoption Authority has identified any pre-defined retention requirements in applicable regulations or laws. Where none exists, we will define internal retention limits based on the specifics of lawful processing.

1. Pre-defined mandatory retention requirements or formal recommendations associated with either the purpose, or the legal basis for processing for example
 - a. Processing of personal data related to the Adoption Authorities statutory functions under the Adoption Act 2010 and the Adoption (Amendment) Act 2017.
 - b. Processing personal data related to financial regulations, tax affairs, or legal proceedings. Retention will reflect government, regulator, revenue, or judicial guidelines.
 - c. Processing personal data for one of the purposes the GDPR exempts from storage limitation under certain conditions, for example scientific research purposes as referenced in GDPR Article 89(1). The Adoption Authority currently does not engage in any scientific research.
 - d. Processing personal data to comply with separate legal requirements, which specify their own retention requirements or exemptions, for example anti-fraud and anti-money laundering requirements.

- e. Processing personal data to service a request made in the public interest by a public authority, for example, to satisfy appropriately authorised national security, or anti-discrimination requirements, where those requirements include a specific retention requirement.
2. The Adoption Authority have internally defined different retention periods for individual processing purposes, having confirmed that processing is lawful and that there is a justification for retaining personally identifiable data to carry out specified processing. That justification has taken into account 2.2.2 (special data categories) and 2.2.3 (data minimisation). These retention periods are set out in the ***Adoption Authority's Records of Processing activity***.

Default personal data retention periods

One or more default retention periods for personal data may be defined by the Adoption Authority's Data Protection Officer and agreed with the *key data protection stakeholders". If no specific retention period has been defined for an individual processing purpose, or a data set cannot be linked to a pre-defined processing purpose, this default retention period will apply.

The default retention period can be extended after consultation with the DPO and *key data protection stakeholders" if it is possible to identify a valid legal basis for on-going data retention or a link the data set in question to a pre-defined purpose with a longer pre-approved retention period.

Any such extension to a default retention period will be noted in the Adoption Authority's Record of Processing activity, together with the name of the authoriser.

*AAI Board & Senior Management team

3 Recording and reviewing retention requirements

Notifying data subjects and internal record keeping

A defined retention limit should be recorded for each data processing purpose. The retention limits will be included in:

- The Adoption Authority Privacy Policy made available to data subjects before their personal data is processed, or if not feasible to include specific time limits, it should include the criteria used to decide upon those limits (Article 18(2)(a));
- The Adoption Authority's Record of Processing Activity (ROPA). Article 30 requires every organisation processing personal data to create and maintain a ROPA. Article 30(1) (f) states that time limits for retention of different categories of data should be included, where possible;
- The Adoption Authority Information Asset Register. The more granular record of individual data collection purposes, associated data sets, and the systems and suppliers linked to data processing.

Where specific retention limits are awaiting clarification for new processing purposes, or, the Adoption Authority is still working to confirm the correct legal basis for processing, the appropriate default retention will be noted with a reminder to ensure it is updated by the accountable data protection stakeholder when specific retention requirements are confirmed.

Review of Retention

Risks to the rights and freedoms of data subjects will evolve over time. Data processing techniques and technologies and data security threats all change rapidly. In addition, where data anonymisation or erasure may not initially be possible without significant impact to other data subjects and wider operations, it may become feasible in the future. Therefore, there will be a periodic review of both the default retention period(s) and specific retention periods linked to individual purposes, or legal bases for processing.

Retention requirements and periods will be reviewed once a year by the Data Protection Officer and *key data protection stakeholders" and at any time following legislative changes relevant to the Adoption Authority and its data.

*AAI Board & Senior Management team

4 Taking action when the retention limit is reached

When the retention period for a data set expires, that personal data will be either:

- Securely deleted from all systems;
- Anonymised so that no individual can be identified by analysis of the anonymised data set, or by pairing that data set with other relatively easy to obtain data;
- Securely physically destroyed (paper records and/or data storage devices);
- Encrypted following current cryptographic best practice, before decryption keys are securely deleted.

Proposals to erase, anonymise, or put data beyond use should be reviewed and signed off by the Board at least 12 months before the end of the applicable retention period. This is necessary to allow time to secure budget and to plan for required changes, or, if necessary, to explore alternatives.

Data treatment at the end of a retention period is a sustainable on-going activity.

Part of that process is creation of an agreed procedure/protocol to review retention periods when data reaches the retention limit each year, month, or each quarter as applicable.

Processor retention requirements

The Adoption Board & Senior Management will formally specify data retention responsibilities in third party and partner contracts, partnership agreements, and service agreements. Each third party that acts as a personal data processor or joint controller must comply with this policy or the terms of their contract and any specific retention requirements linked to different data processing purposes.

Managing retention policy exceptions

*Key data protection stakeholders” will be informed if retention requirements cannot be met for any reason. The potential impact on data subjects for a specified period of non-compliance or for indefinite non-compliance will be assessed and included in a formal application for an exception.

The Data Protection Officer cannot authorise an exception on behalf of the Adoption Authority, nor be held accountable for any associated risk. Only the Adoption Authority’s *key data protection stakeholders “can authorise exceptions and the associated risks on behalf of the Adoption Authority.

The role of the Data Protection officer is to ensure that the “key data protection stakeholders” in the Adoption Authority understand regulatory requirements, and the potential risks associated with non-compliance to inform their decision-making.

*AAI Board & Senior Management team

5 Disposal of Records

All disposal of records will be carefully reviewed; ill-considered disposal is to be avoided at all costs.

Disposal of documents should not be commenced without firstly consulting with the CEO & Data Protection Officer.

It is vital that the process of record disposal safeguards and maintains the confidentiality of the records. This can be achieved internally or via an approved records shredding contractor, but it is the responsibility of the Adoption Authority to satisfy ourselves that the methods used provide adequate safeguards against accidental loss or disclosure of records.

What is Confidential?

Any records containing personal identifiable information such as name, address, date of birth, PPS number, employee number, or medical information is deemed confidential. Other records may be deemed confidential if they contain information about AAI business or finances. Such documents include financial records, payroll records, personnel files, legal documents or medical reports.

Segregation of confidential waste

Documents that are confidential will be disposed of in confidential clear waste bags (available from Corporate Services). Recycling bins and shredding machines are available for non-confidential paper/magazines/circulars. There are two confidential waste options available to staff: On-site shredding or shredding by an approved waste contractor.

- The Adoption Authority staff are encouraged to shred confidential records into confetti-like particles using in-house shredders. This shredded paper can be recycled as part of a recyclable collection.
- Bags of confidential records can also be collected for shredding in a shredding contractor's vehicle on site. These may be shredded off site at an agreed location after consultation with Corporate Services.

If any personal data is inadvertently disposed of; the terms of the Breach Management Policy apply and the DPO must be notified immediately.

Review of Disposal

Disposal requirements and methods will be reviewed once a year by the Data Protection Officer and *key data protection stakeholders" and/or at any time following legislative changes relevant to the Adoption Authority and its data. Medical records held by the Medical advisor will be disposed of bi-annually in a prescribed manner.

*AAI Board & Senior Management team