	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

RECOMMENDATION ON DATA RETENTION AND DESTRUCTION

July, 2024 Written by Security & Privacy Committee

1. Background

WMDA is committed to ensuring the integrity and security of its members' business information alongside their own. This recommendation outlines the procedures and standards that member organisations are expected to follow concerning the retention and destruction of personal data. The aim is to protect individuals' rights and freedoms and ensure full compliance with the data protection principles outlined in the General Data Protection Regulation (GDPR).

This recommendation sets out guidelines for retaining personal data, specifying how long different types of data should be kept and under what circumstances they should be deleted. It also outlines measures to ensure personal data is stored securely during its retention period, such as specifying the type of encryption or access controls that need to be implemented. **This is a high-level overview as the member's policy should be drafted taking into account each one's national legal/regulatory requirements.**

In addition to retention guidelines, this recommendation provides guidance on data destruction methods, such as shredding or secure deletion using software tools. It also specifies the frequency and circumstances for data destruction.

Overall, the purpose is to ensure personal data is handled responsibly and compliantly, safeguarding individuals' rights and freedoms and protecting member organisations and WMDA from potential legal and reputational risks associated with mishandling of personal data.


2. Legal Context

The General Data Protection Regulation (GDPR) has a broad territorial scope designed to protect the personal data of individuals within the European Union (EU). Its provisions apply not only within the EU but also extend to organisations outside the EU that process personal data of EU residents. This has significant implications for international registries, including international WMDA members, and their data exchanges with other members directly subject to GDPR.

Territorial Scope of GDPR

The GDPR applies in the following scenarios:

- 1. EU Establishments (Article 3(1)):** The regulation applies to all organisations established in the EU that process personal data, regardless of where the data processing takes place. This means that any WMDA member based in the EU must comply with GDPR when processing personal data.
- 2. Non-EU Establishments (Article 3(2)):** GDPR also applies to organisations outside the EU if they:

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- Offer goods or services (even for free) to individuals in the EU.
- Monitor the behaviour of individuals in the EU.

Implications for International Registries

International registries that exchange data with WMDA and other members directly subject to GDPR must consider the following:

1. Data Transfers:

- **Adequacy Decisions (Article 45):** Personal data can be transferred to non-EU countries if the European Commission has determined that the country ensures an adequate level of data protection.
- **Appropriate Safeguards (Article 46):** In the absence of an adequacy decision, data transfers can still occur if appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) (incorporated into WMDA's DUA).

2. Compliance Requirements:

- **Controller and Processor Obligations:** International registries acting as data controllers or processors must comply with GDPR principles, such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.
- **Contracts and Agreements:** The WMDA's DUA must be in place between WMDA, its members, and any third-party processors, outlining GDPR compliance obligations.


3. Data Subject Rights:

- **Right to Information and Access (Articles 13-15):** Individuals have the right to know how their data is being processed and to access their data.
- **Right to Rectification and Erasure (Articles 16-17):** Individuals can request corrections to their data or its deletion under certain conditions.
- **Right to Restriction and Objection (Articles 18-21):** Individuals can request limitations on data processing or object to processing activities.

Thus, the GDPR provides a legal framework for the retention of personal data. Under GDPR, personal data must be processed lawfully, fairly, and transparently, with processing limited to what is necessary for specific purposes. **This means personal data should only be retained for as long as needed to achieve the purpose for which it was collected.**

Article 5(1)(c) of GDPR states that personal data shall be "adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed" (data minimisation).

Article 5(1)(e) of GDPR requires that personal data be kept in a form that permits the identification of data subjects no longer than necessary for the purposes for which it is

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

processed. Additionally, GDPR mandates appropriate technical and organisational measures to ensure the security of personal data during its retention period.

GDPR also grants individuals rights regarding their personal data, including the right to erasure (the "right to be forgotten"). This means individuals can request their personal data be deleted in certain circumstances, such as when it is no longer needed for its original purpose or when consent is withdrawn.

3. High-Level Requirements (Governance)

Implementing a data retention programme within member organisations involves several operational steps:


- **Identify the Types of Data:** Identify the types of personal data collected, processed, and stored to determine the retention periods for each type (Personal data discovery).
- **Determine Retention Periods:** Based on the purpose for which the data is collected and any legal or regulatory requirements, determine and document retention periods for each type of data in a data retention policy (Personal data retention schedules/matrix) and include them in the Records of Processing Activities (ROPA) as required by Article 30(1)(f) GDPR.
- **Develop Data Retention Policy:** Specify retention periods, procedures for managing data during the retention period, and secure disposal methods once the retention period expires. Include measures for secure storage during retention.
- **Implement the Policy:** Communicate the policy to all relevant stakeholders within the organisation.
- **Monitor Compliance:** Regularly monitor compliance with the data retention policy through audits and reviews to identify non-compliance areas and improve the data retention programme's effectiveness.
- **Review and Update:** Regularly review and update the data retention policy to ensure it remains current with any legal or regulatory changes and reflects the organisation's data processing activities.

4. Responsibilities as Data Controller

Under GDPR, personal data should not be kept longer than necessary for its original purpose. As data controllers, member organisations must ensure compliance with data protection principles, including storage limitation, and must instruct their data processors, such as WMDA, accordingly.

The Data Retention and Destruction Policy ensures compliance with storage limitation and data subject rights. Data controllers must secure personal data during retention with appropriate technical and organisational measures.

When receiving a request to delete a data subject's data, the following steps must be taken by the data controller:

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- **Verify the Request:** Ensure the erasure request is authorised by the data subject and verify their identity.
- **Review the Data:** Identify all personal data held for the data subject across systems and include all copies in the deletion process.
- **Notify WMDA:** Inform WMDA (acting as the data processor) of the erasure request and provide clear instructions for data deletion.
- **Delete the Data:** Instruct WMDA to securely delete the data subject's data in accordance with the data retention and destruction policy.
- **Confirm Deletion:** Confirm with WMDA that the data has been deleted and request evidence if required.
- **Record Keeping:** Maintain records of the deletion process, including date, time, method, and evidence of secure deletion.

Article 28 of GDPR mandates that data processors must act only on the documented instructions of the data controller, which includes processing and deleting data as per the controller's requests and ensuring compliance with GDPR.

5. Example of Data Retention Schedule for a Donor


A data retention schedule for a stem cell donor in an international registry depends on regulatory requirements, the national law of the member registry, the registry's specific needs, and individual donor circumstances. An example schedule may include:

- **Donor Contact Information:** Retained for a minimum of 15 years following recruitment to allow contact in case their stem cells are needed for a transplant.
- **Medical Information:** Retained for a minimum of 10 years following recruitment, including health status, medical history, and test results.
- **Consent Forms:** Retained for a minimum of 10 years following recruitment to provide evidence of informed consent.
- **Stem Cell Donation Records:** Retained for a minimum of 30 years following donation, including date, location, and recipient identity.
- **Personal Identifying Information:** Retained for a minimum of 15 years following recruitment to locate the donor if needed.

Retention periods should be tailored to each registry based on regulatory requirements, specific needs, and relevant factors, such as domestic legislation.

6. Technical Methodology

Implementing a retention and destruction policy for structured and unstructured data requires technical measures and operational processes:

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- **Identify Data Sources:** Identify all sources of structured and unstructured data within the organisation.
- **Classify Data:** Classify data based on type and sensitivity to determine retention periods and destruction methods.
- **Set Retention Periods:** Establish documented retention periods for each data type in the retention and destruction policy.
- **Define Access Controls:** Implement access controls for each data source to ensure only authorised personnel can access personal data.
- **Develop Deletion Plan:** Create a plan detailing data source, specific data for deletion, retention period, deletion method, date and time, and responsible person.
- **Execute the Deletion:** Perform deletion as per the plan using automated tools or manual methods.
- **Verify Deletion:** Confirm successful deletion through audit logs or test restores.


Alternatively,

- **Automated Retention and Destruction:** Use automated tools to enforce the retention and destruction policy, automatically deleting data when the retention period expires.
- **Monitor Compliance:** Conduct regular audits to ensure policy compliance and address deviations.
- **Secure Data Destruction:** Use secure methods for data destruction, such as software tools or physical shredding.
- **Document Data Destruction:** Maintain records of data destruction activities, including date, time, method, and evidence of secure destruction.

7. Data Retention Policy (Example)

This data retention policy outlines retention periods for various types of personal data:

- **Purpose:** Provide guidelines for the retention and destruction of personal data in compliance with GDPR under WMDA's DUA.
- **Scope:** Applies to all personal data processed by member organisations, whether electronic or paper format.
- **Retention Periods:**
 - **Health Records / data shared via WMDA:** Retained for a minimum of X years following the last treatment date.
- **Data Destruction:**
 - **Electronic Data:** Securely deleted using software tools that overwrite data to prevent recovery.

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

- **Paper Records:** Securely shredded and disposed of to ensure they cannot be reconstructed.
- **Record Keeping:** Maintain records of data retention and destruction activities, including deletion date and time, method used, and evidence of secure destruction.
- **Compliance Monitoring:** Conduct regular audits and reviews to ensure policy compliance and identify improvement areas.

8. Notes

This example data retention policy should be tailored to the organisation's specific needs, national laws, and GDPR principles, especially data minimisation.

This recommendation is not a policy or standard but a guide to be used where national or institutional regulations are lacking.

Member organisations are expected to ensure that examples align with WMDA standards and the Data Use Agreement (DUA), and clarify IT service provider roles, balancing operational stress and allowing time for change management.

Member organisations are expected to differentiate between donor data erasure under the application of retention schedules and data minimisation procedures within the organisation, and the "right to erasure," which requires explicit notification from the member (data controller) to WMDA for complete data removal in response to the data subject's "right to erasure" requests.

9. Glossary

Data Controller: The entity (organisation, company, or individual) that determines the purposes and means of processing personal data.

Data Processor: An entity that processes personal data on behalf of the data controller, following their instructions.


Personal Data: Any information relating to an identified or identifiable natural person, such as names, email addresses, IP addresses, and more.

Data Subject: The individual whose personal data is being processed.

Data Protection Officer (DPO): A designated individual responsible for overseeing data protection strategies and ensuring compliance with GDPR within an organisation.

Consent: A freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data.

Data Breach: A security incident where personal data is unlawfully accessed, disclosed, lost, or destroyed.

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

Subject Access Request (SAR): A request made by a data subject to obtain access to the personal data held about them by a data controller.

Right to Erasure (Right to be Forgotten): The right of individuals to have their personal data deleted by the data controller when it is no longer necessary or if they withdraw consent.

Data Portability: The right of a data subject to receive their personal data in a commonly used, machine-readable format and to transfer that data to another controller.

Legitimate Interest: A lawful basis for processing personal data, where processing is necessary for the legitimate interests of the data controller or a third party, provided that the data subject's rights are not overridden.

Processing: Any operation performed on personal data, including collection, storage, use, disclosure, and deletion.

Pseudonymisation: The processing of personal data in such a way that it can no longer be attributed to a specific data subject without additional information.


Supervisory Authority: An independent public authority established by a member state to oversee GDPR compliance, such as the Information Commissioner's Office (ICO) in the UK.

Data Protection Impact Assessment (DPIA): A process to identify and mitigate risks related to the processing of personal data, particularly when introducing new data processing technologies or methods.

Structured Data: Data that is organised in a pre-defined manner, often in databases or spreadsheets, making it easily searchable and analysable. Examples include names, addresses, and numerical data stored in a table.


Unstructured Data: Data that does not have a pre-defined format or structure, making it more difficult to search, analyse, and process. Examples include emails, images, videos, and text documents.

Technical and Organisational Measures: Security and governance practices implemented to ensure the protection of personal data. Technical measures may include encryption, access controls, and secure backups, while organisational measures involve policies, procedures, staff training, and data protection protocols.

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

Appendix I: Checklist

My organisation has signed the 2022 WMDA Data Use and Transmission Agreement.	<input type="checkbox"/>
My organisation has documented its technical and organisational measures to secure personal data.	<input type="checkbox"/>
My organisation has identified all collected, processed and stored personal data types.	<input type="checkbox"/>
My organisation has assigned appropriate retention periods for each personal data type.	<input type="checkbox"/>
My organisation has a data retention schedule.	<input type="checkbox"/>
My organisation has a data retention policy.	<input type="checkbox"/>
My organisation has a policy or procedure on handling a data subject's request for data erasure.	<input type="checkbox"/>
My organisation has a process to provide access privileges based on user roles and responsibilities.	<input type="checkbox"/>
My organisations maintains records of data destruction activities.	<input type="checkbox"/>
My organisation has a data retention and destruction deletion plan.	<input type="checkbox"/>
My organisation has a data retention and destruction policy.	<input type="checkbox"/>
My organisation regularly reviews and updates its data protection policies to comply with current regulations	<input type="checkbox"/>
My organisation has a designated Data Protection Officer (DPO) or equivalent responsible for data privacy compliance.	<input type="checkbox"/>
My organisation has implemented encryption and other security measures for data in transit and at rest.	<input type="checkbox"/>
My organisation has a procedure for responding to data subject access requests (DSARs) within the required timeframe	<input type="checkbox"/>
My organisation maintains an inventory of all data processing activities, including third-party processors.	<input type="checkbox"/>

	Recommendation on Data Retention and Destruction		
	Document type	Recommendation	Drafting date
	Document reference		Approved by
	Version	1	Approval date
	Drafting date	July, 2024	Status

Appendix II: Example of Data Retention Schedule

TYPE OF DATA	RETENTION PERIOD	REASON	COMMENTS
Visitor logs.	[6 months]	Best practice	No set period in law but as these can contain personal data, should be kept for no longer than is necessary for the purpose.
Accounting records.	-3 years from the date they were made (private company) -6 years from the date they were made (public company)	Section 388(4) Companies Act 2006 (CA 2006)	Tax requirements or other legislation may require longer.
General information about internally developed IT infrastructure, software and systems for internal use.	[5 years from decommissioning of system]	Business need	No statutory period so organisation can balance need to retain these records against data minimisation principle.
System backups.	[3 months]	Business need	May be different depending on the system.
Insurance claims	3 years after settlement	Limitation period	