

Data retention and destruction policy

In adherence to the principles of transparency, accountability, and privacy, the World Marrow Donor Association (WMDA) has established a comprehensive Data Retention Policy as an integral component of its Terms of Use. This policy outlines the guidelines and procedures governing the retention, storage, and disposal of user data collected through the WMDA platform.

Purpose of Data Retention:

The primary objective of data retention within the WMDA framework is to facilitate the efficient operation of the organization's services and to support its mission of connecting donors and patients worldwide. Retained data is utilized for communication, research, and statistical analysis aimed at enhancing the effectiveness of the WMDA's operations.

Types of Retained Data:

WMDA may collect and retain various types of user data, including but not limited to personal information, medical information, communication history, and donor/patient matching details. The organization ensures that the collection and retention of such data are conducted in compliance with relevant data protection regulations.

Retention Period:

Data will be retained for a period deemed necessary for the fulfilment of WMDA's operational objectives, legal obligations, and the provision of ongoing services. The retention period may vary based on the nature of the data, its relevance, and the applicable legal requirements.

The table below describes the retention periods for some of the various WMDA services.

Service	Data type	Retention period
- Search & Match - Patient - Search API	Patient information	42 days + 6 months of no user interaction with patient or its searches: the patient is anonymised by replacing the patient ID with a random string and the birth date with birth year. Patient is no longer accessible by any organisation, except for WMDA admins.
	Search results information	Search result are removed when the patient is "inactivated" (set to the "STP" status). Statistical data regarding number of search results and type of search are retained for analysis purposes.
	Logs regarding API and website use and associated error messages.	Up to 3 years.
Connect API	Encrypted message contents for non-retrieved messages	Messages are available for retrieval for 90 days. After that they are marked as "retrieved" and handled as such. See below for information on retention and destruction information on "retrieved" messages.
	Encrypted message contents for retrieved messages	In order to facilitate recovery of retrieved messages, these messages are retained for 72 hours after retrieval.
	Logs regarding message sending and retrieval. Contains meta information on messages, such as the sending and receiving organisation and validation information.	Up to 3 years.

Security Measures:

WMDA utilizes standard security measures and encryption practices to protect stored data from unauthorized access, disclosure, alteration, or destruction. The organization is dedicated to upholding the confidentiality and integrity of user information through the implementation of encryption, access controls, and regular security assessments. It's important to note that while these measures are industry-standard, no system is entirely foolproof. As such, we cannot offer absolute guarantees regarding the security of the data. WMDA cannot be held responsible for any breaches or data loss. You can contribute to the safety of the system by using strong passwords, proper device security and by not sharing your passwords.

Access and Rectification:

Users have the right to access their personal data stored by WMDA and rectify any inaccuracies. The organization will provide mechanisms for users to review and update their information, ensuring that the data retained remains accurate and up-to-date.

Data Disposal:

Upon expiration of the designated retention period or upon request for deletion by the user (where applicable), WMDA will systematically dispose of data in a secure and irreversible manner. This process will adhere to industry best practices and legal requirements to ensure the permanent removal of user information from WMDA's systems.

Compliance with Applicable Laws:

The data retention practices of WMDA will consistently align with the requirements of relevant data protection laws and regulations, ensuring a legal and ethical framework for the collection, storage, and processing of user data.

By adhering to this Data Retention Policy, WMDA aims to balance the necessity of retaining information for operational purposes with the commitment to safeguarding user privacy and maintaining the highest standards of data protection. This policy is subject to periodic review and updates to align with evolving legal standards and organizational needs. Users are encouraged to review this policy regularly to stay informed about how their data is managed within the WMDA ecosystem.