PathwAI

Data Retention Policy

Version 1 - Approved by Abdullah Adeeb

Contents

1. Objective

Customers and users of PathwAI Labs may request the deletion of data that belongs to them from our systems. This policy outlines the provisions we provide for such requests and describes how such requests should be handled.

2. Scope

This policy applies to data that is in possession of PathwAI Labs and received from our customers or users. Data collected concerning PathwAI Labs products or services that are in testing, alpha/beta state, or an early access program are also part of the scope.

3. Policy Statement

Data retention is based on valid reasons, and customers can request the deletion of their information. Requests should be authenticated and evaluated for legitimacy. Deletion may be withheld if it disrupts services. Anonymization of personal data may be considered before deletion, except where prohibited.

4. Data Retention and Deletion Guidelines

- All data is retained within our systems only when there is a continued and valid reason to store or process the data.
- Customers and users have the right to request the deletion of their information by making a request in writing and including sufficient identification details to validate the requestor's identity.
- **Data Retention Guidelines**:
    - Implement a data classification scheme to categorize data based on its sensitivity and establish a clear retention schedule outlining specific retention periods for different types of data, ensuring compliance with legal and regulatory requirements. Regular reviews and audits should be conducted to identify and securely dispose of data that is no longer necessary.
    - Requests for deletion will be evaluated for authenticity and legitimacy. For example, after a customer has canceled their contract with PathwAI Labs and requested data deletion, we will comply with such a request. However, deletion requests from customers with active contracts may be deemed invalid, as such actions could disrupt services.
- **Data Deletion Guidelines**:
    - Data deletion is initiated upon the termination of service, the end of the data retention period as outlined in the customer agreement, or at the customer’s request. Data will be deleted when it is no longer necessary for the purpose for which it was collected or when the customer requests deletion, provided that the request complies with our

evaluation criteria. Deletion will not be executed if it is determined that retention of the data is necessary to fulfill legal obligations, resolve disputes, enforce agreements, or for legitimate business purposes.

- Data will be permanently deleted from cloud storage, databases, and backups using secure deletion protocols (e.g., cryptographic erasure or overwriting techniques) to prevent recovery. Data from backup systems will be purged according to the backup retention policy agreed upon with the customer. As per the contractual obligations, one-time export may be shared with the customer in the format agreed.
- After the deletion is completed, a confirmation report will be provided to the customer upon request. Implementation teams must ensure adherence to the deletion timelines as per the customer's agreement and adherence to legal and regulatory requirements. When deleting personal data, the company may consider anonymization as an alternative where applicable, provided it does not conflict with any local laws or customer contracts.
- A record of all deletion requests and actions taken shall be maintained for accountability and compliance verification purposes.
- All versions of company policy documentation and older versions will be maintained for at least six years.

5. Document Security Classification

Company Internal (please refer to the Data Classification policy for more details).

6. Non-Compliance

Compliance with this policy shall be verified through various methods, including, but not limited to, automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, which may include termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

7. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

8. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Data Retention Policy. For version history, please see the next page.

Version History

	Version	Log	Date
1	Current	Policy version approved by Abdullah Adeeb	02 Dec, 2025
1		New policy version created	02 Dec, 2025