Data Retention Policy

Version 8

REZOLVE.ai

Document Information

Nameof the document	Data Retention Policy
Release date	11-Dec-2018
Ownedby	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	Initially Drafted
2	11-Dec-2018	Final
3	14-Dec-2020	Review and no change
4	06-Dec-2021	Review and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Review and no change
7	12-July-2024	Updated Document Information
8	23-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022

Reviewer and Approver

Name	Title	Comments	Date
Mr.Udaya Bhaskar Reddy	Co-Founder&CTO	Approved	24-Mar-2025

Contents

1. Purpose and Scope

1.1 Purpose

The objective of the Data Retention Policy is to provide guidance on the retention of the various types of data Rezolve.ai holds. This document strives to balance the need to store information with legal obligations to safely dispose of data when it is no longer required.

This policy is an established protocol for retaining information for operational and regulatory compliance in electronic format (soft copy). It ensures that all Rezolve.ai data managed by the IT team is retained and disposed of in compliance with legal, regulatory, and business requirements.

1.1.1 GDPR Requirements

The General Data Protection Regulation (GDPR) mandates compliance with the principles of **data minimization** and **storage limitation**. This means personal data must 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.”

1.2 Scope

- This policy covers all data related to Rezolve.ai’s products and operational processes.
- **Customer-provided data** is governed by contractual terms agreed upon with the customer.
- The policy applies throughout the **entire data lifecycle** — from creation, storage, and usage to disposal.
- It applies to **all Rezolve.ai staff** and **external users** associated with the company.

2. Policy Standards

2.1 Retention

- This policy helps departments understand their obligations regarding internal and external data retention requirements, including electronic documents.
- Rezolve.ai shall archive, retain, and dispose of data owned or managed by the IT team according to legal, compliance, and business needs.
- Archived data shall be retained securely with clear management practices to ensure easy retrieval and compliance with law.

Confidential/Sensitive Data: Customer information is treated as confidential and must only be stored in protected containers such as centralized File Services, SFTP, and application databases.

2.2 Customer Data & Records

- Customer data shall be retained as per the customer's contract (MSA and/or SOW) or specific customer requests.
- If the contract does not specify, data will be retained for **1 year post termination** of the agreement.
- Upon request, data shall be retained until the customer acknowledges its receipt.

2.3 Personal Data

- Personal data should be retained **only as long as necessary**.
- Retention decisions must consider:
    - Legal obligations for specific data.
    - Whether the original purpose of data processing still applies.
    - Withdrawal of consent or completion/impossibility of the contract.

Determining Retention Periods

Following a **risk-based approach** under the GDPR's accountability principle, Rezolve.ai shall:

- Define and document data retention periods.
- Justify periods as part of its privacy accountability program.
- Be audit-ready with clear criteria for retention timelines.

2.4 Company Data

- Internal company data must be retained to meet legal, regulatory, and operational needs.
- Any disposal or retention actions must be **approved** by the:
    - Data Owner
    - Delivery Head / Project Head / Client Relationship
    - Legal & Compliance Team

2.5 Retention Periods

- Retention periods for various types of data are outlined in **Annexure A**.
- All retention periods are approved by the **Privacy Committee**, **CEO**, or **DPO**, and reviewed periodically.

2.6 Expiration of the Retention Period

After retention expiry, personal data should ideally be **anonymized**, not necessarily deleted. Methods include:

- Removing unique identifiers
- Erasing identifiable elements
- Separating identifying from non-identifying data
- Aggregating data to prevent individual identification

Note: These apply only to **Personal Data (PII)** — not other confidential or strictly confidential information.

2.7 Destruction and Data Disposal

- Data destruction is a critical part of data lifecycle management.
- The **IT department** is responsible for deleting or securely destroying electronic records.
- Destruction should occur **promptly** after data expires and not involve data linked to:
    - Ongoing investigations
    - Audits
    - Litigation
- Managers are responsible for executing destruction plans **annually**.
- Approved destruction methods for non-electronic data include **shredding**.

2.8 GDPR Obligations to Data Subjects

Per GDPR, data subjects must be informed of:

- The **retention period**, or
- The **criteria used** to determine that period, and
- **Updated retention timelines** if data processing purposes change

This must be communicated clearly in the privacy notice for customers, employees, and vendors.

2.9 Destruction Log

A destruction log must be maintained to document each data destruction event, including:

- Date of destruction
- Name of the individual responsible
- Name of the witness
- Method of destruction

2.10 Destruction/Erasure in Accordance with GDPR

Erasure or destruction of GDPR-governed personal data must align with Rezolve.ai's internal privacy and data protection policies.

3. Annexure A – Approved Retention Periods

Non-Personal Data

Type of Data	Retention Period
Client contracts and agreements	3 years from expiry of contract
Client data in applications	As per client contracts
Employee data	As per statutory limits
Accounting and finance-related data	As per statutory limits

Personal Data

Type of Data	Retention Period
Client-provided data through SaaS	Managed by the client through the software
Deletion of data of employees who left	Responsibility of the client to delete the user's PII
General personal data	1 year post termination of the contract

- **Next Review Cycle**: March 2026
- Management may review and revise this policy at any time depending on business or regulatory changes.

Note: All documents referencing *Actionable Science* are considered equivalent to **Rezolve.ai**.