Data Protection Policy and Framework

Version 9

REZOLVE.ai

Document Information

Name of the document	Data Protection Policy and Framework
Release date	24-Dec-2018
Owned by	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

VersionNo	VersionDate	DetailsofChange
1	13-Nov-2018	Initially Drafted
2	10-Dec-2018	Final
3	20-July-2021	Review and no change
4	03-Dec-2021	Review and no change
5	04-Mar-2022	Updated Document Information
6	02-Mar-2023	Review and no change
7	22-Jul-2024	Updated Document Information
8	24-Mar-2025	Updated the document details as per migration from ISO 27001:2013 to ISO27001:2022
9	08-May-2026	Review and no change

Reviewer and Approver

Name	Title	Comments	DateReviewed
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	13-May-2026

Table of Content

1. **Introduction**
   Data protection is safeguarding of the rights of individuals in relation to the processing of personal data, in both paper and electronic format.
   As Rezolve.ai conducts business in the European Union, Rezolve.ai requires to comply with the General Data Protection Regulation (GDPR) on collection, processing, use and disposal of personal data and sensitive personal data.
   In its everyday business operations, Rezolve.ai makes use of variety of data about identifiable individuals, including data about:
   Current, past and prospective employees
   Customers
   Users of its websites
   Subscribers
   Other Stakeholders
   In collecting and using this data, the organization is subject to a variety of legislation controlling how such activities may be carried out and the safeguards that must be put in place to protect it.

Purpose
The purpose of this policy is to set out the relevant legislation and to describe the steps Rezolve.ai is taking to ensure that it complies with it.
The policy helps to protect the rights and privacy of individuals in accordance with GDPR. The policy also sets out the process and the framework within which to collect, use and protect Personal and Sensitive Data.

Scope
The control applies to all systems, people and processes that constitute Rezolve.ai's information systems including Board members, Directors, Employees, Suppliers and other third parties who have access to Rezolve.ai's systems.

List of Referenced Privacy Policy and Procedures
The following policies and procedures are incorporated by reference and relevant to this document:
Data Protection Impact Assessment Process
Data Breach Procedure
Personal Data Mapping Procedure
Legitimate Interest Assessment Procedure
Information Security Incident Response Procedure
GDPR Roles & Responsibilities
Records, Retention and Protection Policy
Change Management Policy

2. Privacy and General Data Protection Policy
   The General Data Protection Regulation
   The General Data Protection Regulation 2016 (GDPR) is one of the most significant pieces of regulation affecting the way Rezolve.ai carries out its information processing activities. Significant fines are applicable

3. if a breach is deemed to have occurred under the GDPR, which is designed to protect the personal data of citizens of European Union. It is Rezolve.ai's policy to ensure that our compliance with the GDPR and other relevant legislation is clear and demonstrable at all times.
4. Definitions
   There are a total of 26 definitions listed within the GDPR and it is not appropriate to reproduce them all here. However, the most fundamental definitions with respect to this policy are as follows:
5. **Data Subject**
   Data subject shall mean the individual in relation to which Rezolve.ai is holding information about; which could be Rezolve.ai employees, clients, customers and other third parties such as contractors, suppliers and agencies.
6. **Personal data**
   Any information relating to an identified or identifiable natural person (‘data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
7. **Processing**
   Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
8. **Controller**
   The natural or legal person, public authority, agency or other body which, alone or jointly with others,

determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

9. **Sensitive Personal Data**
   Sensitive Personal Data shall mean personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceeding. Rezolve.ai does not accept, store, process or transmit any sensitive personal data.
10. **Data Controller**
    A Data Controller is an identified employee within Rezolve.ai who is authorized by Rezolve.ai management to control the collecting, storing, transmitting and using personal information within Rezolve.ai, as per the GDPR. Roles and responsibilities of Data Controller is listed in this policy.
11. **Data Processor**
    A Data Processor is an identified employee within Rezolve.ai who is authorized by Rezolve.ai management to process personal data as instructed by a data controller (which can be the client of Rezolve.ai) for specific purposes as defined by the data controller.

Apart from a Data Controller and Data Processor, Rezolve.ai shall also identify a staff with similar roles and responsibilities of a DPO, to discharge Rezolve.ai obligations under the GDPR. This individual shall be named as a Data Privacy Officer.

Data Controller
Rezolve.ai is not data controller as it does not control the personal information on its Information Assets or in structured manual files. The clients remain the controller for their data.
The key responsibility of a controller is to be accountable and to take actions in line with legal and regulatory requirements, and to be able to explain the compliance of Rezolve.ai with GDPR to its data subjects and the Supervisory Authority, as and when required.

Data Processor
Rezolve.ai is the data processor when it processes data on behalf of a data controller (when data is provided by a client). Data processors are also referred to as third party. The key responsibility of the processor is to ensure that conditions specified by the data controller are always met, and that obligations stated in GDPR are complied with.

Data Privacy Officer
Rezolve.ai does not have an obligation to appoint a Data Protection Officer as:

- Rezolve.ai is not a public authority
- Core business activities of Rezolve.ai does not require large scale, regular and systematic monitoring of individuals such as online behaviour tracking etc.
- Core business activities of Rezolve.ai does not require large scale processing of special categories of data or data relating to criminal convictions and offences.

However, Rezolve.ai shall identify a staff with similar roles and responsibilities of a DPO, to discharge Rezolve.ai obligations under the GDPR. This individual shall be named as a Data Privacy Officer.

2. Privacy Governance
   Quarterly Privacy Meetings
   DPO
   The Data Protection Officer (DPO) is a mandatory requirement required by GDPR. This role is mandatory for organizations that:

- Are a public authority
- Carries out large scale, regular and systematic activities that monitor individuals (for example, online behaviour tracking) to achieve its business objectives
- Carries out large scale processing of special categories of data or data relating to criminal convictions and offences.

DPOs are responsible to assist organizations to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.
Data Protection Officers are not applicable for Rezolve.ai.

Privacy Officer

Data Privacy Officer is an identified employee within Rezolve.ai who is authorized by Rezolve.ai management to carry out its obligations under GDPR. The Data Privacy Officer will have similar roles and responsibilities of a DPO, to discharge Rezolve.ai obligations under the GDPR.

1. Principles Relating to Processing of Personal Data
Six Principles of GDPR
There are a number of fundamental principles upon which the GDPR is based. The legislation places a responsibility on every data controller to process any personal data in accordance with the following principles:

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
5. 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');
6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Rezolve.ai will ensure that it complies with all of these principles both in the processing it currently carries out and as part of the introduction of new methods of processing such as new IT systems.

Specifics about Important Principles
Transparency and Fairness - Privacy Notice
The new regulatory environment demands higher transparency and accountability in how companies manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use. The GDPR contains provisions that Rezolve.ai shall need to be aware of as data controllers, including provisions intended to enhance the protection of our customer's personal data.

Regarding Data Collection, Rezolve.ai is not a data collector, the customer is the data collector. The data controller is the customer of Rezolve; they are responsible for collection and providing information.

Privacy notices are written in a clear, plain way that our customers shall understand.

Any forms used to gather data on an individual shall contain a statement (fair collection statement) explaining the use of that data, how the data may be disclosed, and also indicate whether or not the individual needs to consent to the processing.

Accuracy and Relevance
Rezolve.ai shall ensure that any personal data processed is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Rezolve.ai shall not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this. Individuals may ask that we correct inaccurate personal data relating to them.

Data Deletion
As per the customer contract, Rezolve will retain and delete the data on the specific events. The events are customer employee or customer leaves.

Data Retention
Rezolve.ai retains personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but if relevant, the length of retention will be determined in a manner consistent with published legal and regulatory data retention guidelines.

2. Rights of the Individual
The data subject also has rights under the GDPR. These consist of:

1. The Right to be informed
2. The Right of Access
3. The Right to Rectification
4. The Right to erasure
5. The Right to Restrict Processing
6. The Right to Data Portability
7. The Right to Object
8. The Right in relation to automated decision making and profiling

Each of these rights are supported by appropriate procedures within Rezolve.ai that allow the required action to be taken within the timescales stated in the GDPR. These timescales are shown in the table below:

Data Subject Request	Timescale
The Right to be informed	When data is controlled (if supplied by data subject) or within one month (if not supplied by the data subject)
The Right of Access	One Month
The Right to Rectification	One Month
The Right to erasure	Without Undue Delay
The Right to Restrict Processing	Without Undue Delay
The Right to Data Portability	One Month
The Right to Object	On receipt of Objection
The Right in relation to automated decision making and profiling	Not specified

Rezolve.ai is data controller.
Rezolve.ai, upon request from a data subject, shall provide a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals.
Rezolve.ai will also allow a data subject request to transfer their data directly to another system.
Rezolve.ai will take one month to provide a full response to the data subject. Data subjects can be encouraged to submit requests during term time but are under no legal obligation to do so.

3. Lawfulness of Processing
There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the GDPR. It is Rezolve.ai's policy to identify the appropriate basis for processing and. **To document it, in accordance with the Regulation. The options are described in brief in the following sections.**

Consent
Rezolve does not act as the Data Controller. Instead, it maintains data provided by the Data Controller through applications hosted by Rezolve. The Data Controller can manage their data via the application or by making explicit requests to Rezolve, which will handle the data accordingly.
Unless it is necessary for a reason allowable under the GDPR, Rezolve.ai will always obtain explicit consent from a data subject to control and process their data.
In case of children below the age of 16 (a lower age may be allowable in specific EU member states) parental consent will be obtained.
Transparent information about our usage of their personal data will be provided to the data subject at the time that consent is obtained and their rights with regard to their data explained, such as the right to withdraw consent. This information will be provided in an accessible form, written in clear language and free of charge.
If the personal data are not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data are obtained and definitely within a month.

Consent as a basis for processing
Rezolve.ai shall ensure that an individual's ‘consent' to process their personal data is accepted explicitly and is freely given, as a specific, informed and unambiguous indication of the individual's wishes. The consent shall be provided by a clear affirmative action, and shall signify an agreement to the processing of their personal data.

The data subject is allowed to withdraw their consent at any time. All consents shall be recorded and stored.
Non-response to a communication shall not be considered as consent.
The Controller shall be able to demonstrate that consent was obtained for the processing operation.
Currently, Rezolve.ai does not process sensitive data. In case sensitive data is being collected, an explicit written consent of individuals shall be obtained unless an alternative legitimate basis for processing exists.

Performance of a contract
Where the personal data collected and processed are required to fulfill a contract with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question. E.g. a delivery cannot be made without an address to deliver to.

2.5.3 Legal Obligations
If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This may be the case for some data related to employment and taxation, for example, and for many areas addressed by the public sector.

2.5.4 Vital Interests of the Data Subject
In a case where personal data are required to protect the vital interest of the data subject or of another natural person, then this may be used as the lawful basis of the processing. Rezolve.ai will retain reasonable documented evidence that this is the case, whenever this reason is used as a lawful basis of the processing of personal data. E.g. this may be used in aspects of social care, particularly in the public sector.

2.5.5 Task carried out in the public interest
Where Rezolve.ai needs to carry out a task that it believes is in the public interest or as part of an official duty, then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

Legitimate Interests
If the processing of specific personal data is in the legitimate interests of Rezolve.ai and is judged not to affect the rights and freedom of data subjects in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

2. Data Mapping and Data Inventory
Rezolve.ai shall maintain a record and maintain a data processing inventory. This is a formal list of the processing activities and their purpose. Rezolve.ai shall ensure that this Data Processing list is aligned with Rezolve.ai business.
Maintaining such a Data processing inventory is a requirement under GDPR article 30.
These records may contain:

- The name and contact details of the controller
- Controller's representative and the data protection officer (if applicable)
- Purposes of the processing
- Description of the categories of data subjects and of the categories of personal data
- Categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations
- Where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, along with the documentation of suitable safeguards
- Envisaged time limits for erasure of the different categories of data
- A general description of the technical and organisational security measures referred to in

3. Data Protection Impact Assessment
Rezolve.ai shall conduct Data Protection Impact Assessment ("DPIA") to identify and minimize the privacy risks of ongoing or new projects or policies, and to ensure that potential problems are identified at an early stage, and to address them at the earliest without any impact to the organization.
Rezolve.ai shall conduct DPIA as defined by Rezolve.ai Procedure for Data Protection Impact Assessment.

Privacy by Design
Rezolve.ai has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The Data Controller shall be responsible for ensuring that all data security processes and projects commence with a privacy plan. When relevant, and when it does not have a negative impact on the data subject, privacy settings shall be set to the most private by default.
The data protection impact assessment will include:

- Consideration of how personal data will be processed and for what purposes;
- Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s).
- Assessment of the risks to individuals in processing the personal data;
- What controls are necessary to address the identified risks and demonstrate compliance with the legislation
  Note: Use of techniques such as data minimization and Pseudonymization will be considered where applicable and appropriate.

4. Technical and Security Measures
Rezolve.ai protects personal data against loss or misuse. When other organisations process personal data as a service on behalf of Rezolve.ai, the Data Controller shall establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third-party organisations.

5. Data Sharing and Cross Border
Rezolve.ai will ensure that all relationships it enters into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

International Transfers of Personal Data
Transfers of personal data outside the EU will be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the EU's judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time.
Intra Group International Data transfers will be subject to legally binding agreements referred to as binding Corporate Rules (BCR) which provide enforceable rights for data subjects.

Data Protection Officer
A defined role of Data Protection Officer (DPO) is required under the GDPR if:

- An organization is a public authority
- It performs large scale monitoring
- It processes particularly sensitive types of data on a large scale.
  The DPO is required to have an appropriate level of knowledge and can either be an in-house resource or outsourced to an appropriate service provider.
  Based on these criteria, Rezolve.ai does not require a DPO to be appointed.

6. Breach Notification
Under the GDPR, it is the responsibility of the Data Controller to report a data breach to the relevant supervisory authority. The Data Controller must notify the regulator without undue delay and, where feasible, within 72 hours after becoming aware of the breach. Rezolve being the Data Processor must inform the Data Controller without undue delay upon becoming aware of a data breach.
This will be managed in accordance with our information security incident response procedure which sets out the overall process of handling information security incidents.
Rezolve.ai has established a formal Data Breach procedure. All staff shall be trained to follow the Data Breach procedures.

7. Addressing Compliance to the GDPR
The following actions are undertaken to ensure that Rezolve.ai complies at all times with the accountability principle of GDPR:

- The Legal basis for processing personal data is clear and unambiguous
- A Data Protection Officer is appointed with the specific responsibility for data protection in the Organization, if required
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Training in Data Protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to Data Subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively.
- Regular reviews of procedures involving personal data are carried out
- Privacy by Design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:
  - Organization name and relevant details
  - Purposes of personal data processing
  - Categories of individuals and personal data processed
  - Categories of personal data recipients

- Agreements and mechanisms for transfers of personal data to Non-EU countries, including details of controls in place
- Personal Data Retention Schedules
- Relevant Technical and Organizational Controls in Place
  These actions are reviewed on a regular basis as a part of the management process concerned with Data Protection.

Training
All Rezolve.ai staff shall receive training on this policy. New joiners will receive training as part of the induction process. Further training shall be provided at least once a year or whenever there is a substantial change in the law or our policy and procedure.
Training is provided through an in-house session on a regular basis. Training shall cover:

- The law relating to data protection
- Rezolve.ai data protection and related policies and procedures.
  Completion of training is mandatory for all staff.

Self-Assessment
Rezolve.ai has established an internal process of review and self-assessment to ensure the confidentiality of our data is maintained and there are stringent controls in place regarding access and use of confidential and personal data. Decisions on data collection and releasing to third parties for processing are subject to detailed assessment and approval by senior management.
Following activities are strictly monitored and reviewed:

- Who is requesting the data
- Purpose for which it is required?
- Category of personal data requested
- Arrangements in place to store and handle the data
- Performance of data processors
  Rezolve.ai shall formally conduct an audit covering areas of data processing such as what data is held, where it is stored, how it is used, who is managing it - and any other data processing activities that may be relevant.

Enforcement

All employees (permanent or temporary) shall comply with the conditions of use set out in this policy.
Breaches of this policy and/or security incidents are defined as events which could have, or have resulted in, the loss, alteration, or unauthorized deletion of personal data of Rezolve.ai customers.

All employees have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Rezolve.ai Incident Reporting Procedure. This obligation also extends to any external organization contracted to support or access Rezolve.ai Information Systems.

If Rezolve.ai becomes aware of any criminal conduct or an alleged breach of this Policy, action shall be taken as stipulated by the GDPR.

2. Annexure – Roles and Responsibilities

Data Controller – Roles and Responsibilities

- When personal data has been collected, provide data subjects with relevant details such as:
  - The purpose of processing the data
  - Recipients of the data
  - Period for which the data will be stored
- When personal data has not been collected directly from the subject, provide the same details above.
- Implement measures to safeguard the data subject's rights to contest decisions based on automated data processing, including profiling.
- Establish appropriate data protection policies.
- Create binding corporate rules to regulate international transfers of personal data and ensure they are approved by the supervisory authority.

- Document any personal data breaches.
- Conduct assessments and implement safeguards prior to transferring personal data to a third country or international organization.
- Adhere to codes of conduct or certification mechanisms to demonstrate compliance with GDPR requirements.
- Implement technical and organizational measures to:
    - Minimize the collection and processing of data
    - Ensure confidentiality, integrity, availability, and resilience of processing systems and services
    - Enable ongoing testing, assessment, and evaluation of data security measures
- Demonstrate compliance with data minimization and protection principles.
- Conduct a Data Protection Impact Assessment (DPIA) when a data processing activity is likely to result in high risk.
- Perform reviews to ensure data processing aligns with DPIAs.
- Conduct data protection audits to verify compliance with binding corporate rules.
- Respond to data subjects' requests:
    - For access to their personal data
    - To lodge complaints with the supervisory authority
    - To rectify inaccurate or incomplete data
    - To exercise the right to be forgotten
    - To restrict processing under specific conditions
    - To be informed of rectification, erasure, or restrictions
    - To object to processing
    - Regarding automated decision-making involving special categories of data
- Notify:
    - The supervisory authority of a personal data breach within 72 hours of awareness
    - Data subjects of personal data breaches without undue delay
- Consult the supervisory authority when a DPIA indicates high risk without sufficient mitigation.
- Ensure Data Protection Officers (DPOs), where appointed, can manage data subject requests.
- Onboard only data processors who can ensure compliance with data protection obligations.
- Implement contracts to govern how data processors handle, store, and process data.
- Ensure restoration of access and availability to personal data quickly in the event of a physical or technical incident.

Data Processor Roles and Responsibilities, **Data Privacy Officer Roles and Responsibilities**, and your **review note** — with improved structure, punctuation, and readability:

Annexure – Roles and Responsibilities (continued)

Data Processor – Roles and Responsibilities

- Adhere to codes of conduct or certification mechanisms to demonstrate compliance with GDPR.
- Conduct assessments and implement appropriate safeguards before transferring personal data to a third country or international organization.
- Implement measures to ensure the confidentiality, integrity, availability, and resilience of processing systems and services.
- Assist the Data Controller in ensuring compliance with GDPR requirements, including audits.
- Ensure ongoing testing, assessment, and evaluation of the effectiveness of data security measures.
- Conduct data protection audits to verify compliance with binding corporate rules.
- Notify the Data Controller of a data breach without undue delay.
- Obtain the Data Controller's approval before engaging another processor.
- Conduct effective due diligence on downstream processors to ensure GDPR compliance.
- Restore availability and access to personal data quickly in the event of a physical or technical incident.

Data Privacy Officer – Roles and Responsibilities

- Protect Rezolve.ai Information Technology assets and ensure their usage aligns with legal and regulatory requirements, as well as internal policies and procedures.
- Inform data controllers and data subjects about their data protection rights, obligations, and responsibilities, and raise awareness.
- Provide advice and recommendations to senior management regarding the interpretation and application of data protection regulations.
- Ensure an inventory of all IT assets is maintained, including:

    - Hardware details
    - Software details
    - Access rights
    - Usage information
- Manage maintenance contracts (as applicable) and related documentation for each IT asset.
- Ensure that a register of processing operations is maintained and that all processing activities comply with GDPR requirements.
- Handle queries or complaints related to Data Privacy or legal/regulatory matters raised by senior management, the Data Controller, or any other stakeholder.
- Collaborate with the Data Controller in case of:
    - Data breaches
    - Investigations
    - Complaint handling
    - Audits
    - Interactions with supervisory authorities
- Escalate to senior management any actual or potential failure to comply with applicable data protection rules.

- **Next Review Cycle**: March 2027
- Management reserves the right to review and update this policy at any time based on business needs or regulatory changes.
- **Note**: All documents referencing *Actionable Science* are to be interpreted as referring to **Rezolve.ai**.