Data Subject Rights
Version 9

REZOLVE.ai

Document Information

Nameof the document	Data Subject Rights Policy
Release date	19-Dec-2018
Owned by	Boopathi
Governed by	Mr.Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	13-Nov-2018	InitiallyDrafted
2	10-Dec-2018	Final
3	15-Dec-2020	Review and no change
4	01-Dec-2021	Review and no change
5	04-Mar-2022	Updated document information
6	02-Mar-2023	Review and no change
7	18-Sep-2024	Updated document information
8	23-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	Date
Mr.Udaya Bhaskar Reddy	Co-Founder&CTO	Approved	13-May-2026

Table of Contents

1. Background and Purpose

1.1 Background

Under the **General Data Protection Regulation (GDPR)** of the European Union (EU), data subjects are entitled to exercise specific rights concerning their personal data, including:

- The right to **restrict** processing of their personal data
- The right to **object** to processing of their personal data
- The right to **withdraw consent** previously given for data processing

1.2 Purpose

These procedures are designed to:

- Provide guidance to help **Rezolve.ai** (the "Company") handle requests received from data subjects exercising their rights under the GDPR.
- Supply the **required forms and templates** to document the Company's actions in response to these requests.

These procedures are **supplemental** to the Company's **Personal Data Protection Policy** and should be read in conjunction with it.

2. Rights under the GDPR

The GDPR grants the following rights to individuals:

1. **The right to be informed**
2. **The right of access**
3. **The right to rectification**
4. **The right to erasure** (right to be forgotten)
5. **The right to restrict processing**
6. **The right to data portability**
7. **The right to object**
8. **Rights related to automated decision-making and profiling**

3. GDPR Response Timelines

Data Subject Request	Timescale for Response
The Right to be Informed	When data is collected (if provided by subject) or within 1 month (if not)
The Right of Access	1 month
The Right to Rectification	1 month
The Right to Erasure	Without undue delay
The Right to Restrict Processing	Without undue delay
The Right to Data Portability	1 month
The Right to Object	On receipt of the objection
Rights related to Automated Decision-Making and Profiling	Not specifically defined under GDPR

4. Key Procedures

4.1 Tracking and Handling Requests

- Rezolve.ai acts solely as a **data processor**; data controllers are the Company's customers.
- Requests received from data subjects must be directed to the **data controller** (customer) for action, unless the Company is authorized to act.

- All such requests must be **logged in an internal tracker** and appropriately **responded to** or escalated.

4.2 Right to Information

Individuals have the **right to be informed** about the collection and use of their personal data. This includes:

- The purpose for processing
- Retention periods
- Sharing and disclosure details

This information—collectively called **"privacy information"**—must be:

- Provided at the time of data collection (if obtained from the subject)
- Provided within **one month** if data is collected from a third-party source
- Concise, transparent, intelligible, accessible, and in clear and plain language

Note: You are not required to provide privacy information if the individual already has it or if doing so involves a **disproportionate effort**.

4.3 Privacy Notice

A **Privacy Notice Checklist** is provided in **Annexure 1** to support the development of comprehensive privacy information.

4.4 Right of Access

Under GDPR Article 15, individuals have the right to:

- Confirm that their data is being processed
- Access their personal data
- Access supplementary information (similar to that provided in a privacy notice)

Note: This right supports transparency and lets individuals verify the **lawfulness of processing**.

- Users can access their data through the application interface, e.g., their **user profile** or **admin dashboard**.
- The right of access must be provided **free of charge**, unless the request is excessive or repetitive—fees are then determined by the **Privacy Officer**.
- All access requests must be fulfilled **within one month**.

Large Volume Requests

When a large quantity of personal data is processed, the individual may be asked to **specify the data they wish to access**, as permitted under **Recital 63** of the GDPR.

Right to Restrict Processing

Data subjects have a right to block or suppress processing of their personal data. The Company must inform data subjects of their right to request the Controller to restrict processing of their personal data, at the time of collecting such personal data.

The Company shall restrict processing of personal data in the following cases:

- Where a data subject contests the accuracy of the personal data, the Company should restrict processing of the data until it has verified its accuracy.
- When the processing is unlawful, but the data subject opposes erasure of the data, and instead requests restriction of its use.
- If the Company no longer needs the personal data for processing, but the data subject requires the data to establish, exercise or defend a legal claim.
- Where a data subject has objected to processing that was based on legitimate interests of the Controller, and the Company is considering whether its legitimate interests override those of the data subject.
- Where the Supervisory Authority has ordered restriction of processing of the personal data.

When processing is restricted, the Company can retain or store the personal data, but cannot further process it, except:

- With the data subject's consent, or
- To establish, exercise or defend a legal claim, or
- For protection of the rights of another person or entity.

If the Controller has disclosed the personal data in question to third parties, it must inform such third parties about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so. The Controller shall also inform the data subject about such third parties if the data subject requests it.

Further, the Company must inform the data subject when it decides to lift a restriction on processing. The Company may restrict the processing of personal data by:

- Temporarily moving the selected data to another processing system
- Making the selected personal data unavailable to users, or
- Temporarily removing published data from a website

On automated systems, the restriction of processing should be ensured by technical means, so that the personal data is not subject to further processing operations, and cannot be changed. The fact that the processing of personal data is restricted should be clearly indicated in the system.

Right to Object to Processing

Data subjects have the right to object to:

- Processing necessary for performance of a task in the public interest or in the exercise of official authority by the Controller, or based on legitimate interests of the Controller
- Processing for purposes of scientific/historical research and statistics
- Direct marketing (including profiling)

This means that data subjects cannot object to processing that is based on their **Consent / Explicit Consent**. However, in such cases, the data subject has a right to **withdraw consent** for processing.

Personal Data Processed for Public Interest Task / Exercise of Official Authority / Legitimate Interests of the Company

The data subject must have an objection on “grounds relating to his or her particular situation”. The Company must stop processing (including profiling) the personal data unless:

- It can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or
- The processing is for the establishment, exercise or defence of legal claims.

Personal Data Processed for Scientific/Historical Research or Statistical Purposes

The data subject must have an objection on “grounds relating to his or her particular situation”. The Company must stop processing personal data unless the processing is necessary for the performance of a task carried out in public

interest.

Personal Data Processed for Direct Marketing Purposes

The Company must stop processing personal data for direct marketing purposes (including profiling to the extent related to such direct marketing) as soon as it receives an objection. There are no exemptions or grounds to refuse.

With regard to (i) and (iii) above, the Company must inform data subjects of their right to object **"at the time of the first communication with the data subject"** and in its **Privacy Notice**. These rights must be explicitly brought to the attention of data subjects and presented clearly and separately from any other information.

Lastly, if the Company offers online services including **information society services**, it must offer a way for data subjects to object online or by automated means.

Right to Withdraw Consent for Processing

Data subjects have the right to withdraw their consent given for processing at any time. However, such withdrawal of consent will apply only on a **prospective basis**, and will not affect the lawfulness of processing already performed based on consent before it was withdrawn.

For processing based on **Consent** or **Explicit Consent**, the Controller must inform data subjects at the time when the personal data is obtained, of the right to withdraw consent at any time. The Company should also make it easy for data subjects to withdraw consent at any time they choose.

Where a data subject withdraws consent to processing, and the Company does not have another legal ground for such processing, the Company will need to **erase the personal data without undue delay**.

Right to Rectification of Personal Data

The GDPR requires that personal data held by a Controller / Processor should be rectified in the following circumstances:

Article 16 – Right to Rectification

- The data subject shall have the right to obtain from the Controller **without undue delay** the rectification of inaccurate personal data concerning him or her.
- Taking into account the purposes of the processing, the data subject shall have the right to have **incomplete personal data completed**, including by means of providing a supplementary statement.

Article 5(1)(d) & Recital 39

- Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or erased **without delay**.

Where the inaccuracy of data comes to the attention of the Company, either through intimation by the data subject (i.e. Respondent) or in any other manner, the Company should take immediate steps either to:

- Rectify the data
- Or if that is not possible,
- Erase the data without delay

With regard to **incomplete personal data**:

For data subjects owned by the Company (users for which the Company is the Controller), such data subjects are encouraged to review & complete their personal data profiles periodically.

As such, any other incompleteness or inaccuracy in user personal data profile is the responsibility of the Processor / Controller who owns the data subject. Where informed by the respective Supplier / Controller, the Company shall take reasonable steps to rectify or erase the inaccurate personal data within its control.

Art 58 (2)(g) - Where the Supervisory Authority has ordered the rectification of personal data.

The Company must rectify the data in its possession.

Further, the Company must inform any Recipients (e.g. other controllers) to whom the personal data has been disclosed as per Article 17(2) and Article 19 below.

Right to Erasure of Data / Right to be Forgotten

Handling request for erasure of Data

All requests from data subjects for Rectification or Erasure of their personal data shall be dealt with by the Company's designated Data Protection Officer.

The Name & Contact Details (phone number & email address) of the Data Protection Officer shall be updated on the Company's website.

Where such requests are received by the Controller / Joint Controller / Controller's Representative / Processor or the Company's Customer Support team or Contact Centre, the data subject should be advised to re-direct the erasure request to the Company's designated Data Protection Officer.

Each of these parties should be specifically informed of this process in writing.

(iv) To avoid confusion, the Company's website should clearly state that requests for Rectification or Erasure of personal data should be addressed to the Data Protection Officer.

Process to erase data Timelines for Rectification or Erasure of Personal Data

The GDPR requires that where Rectification or Erasure of personal data is required, such data should be rectified or erased "without delay" or "without undue delay". The Controller has an obligation to erase personal data "without undue delay", in cases specified in Article 17(1).

Within the Company - Rectification or Erasure of data should be completed within 3 weeks from the date of receipt of the request from the data subject.

Outside the Company - Where there is a requirement to notify other parties (e.g. Recipients, other controllers) to whom the personal data has been disclosed under Article 19, such parties shall be notified within 2 weeks from the date of receipt of the request from the data subject.

If a delay is anticipated in meeting the timelines above, the data subject shall be duly informed, together with the date by which the above activities are expected to be completed.

Communicate to data subject

Once the personal data has been Rectified or Erased as per the data subject's request, the Company shall inform the data subject that the request has been duly completed.

Exceptions for Erasure of data

Recital 68 of the GDPR inter-alia provides that the data subject cannot exercise the right to erasure to seek erasure of personal data which was provided by him or her for the performance of a contract, for as long as such personal data is necessary for the performance of such contract.

Article 17(3) and Recital 65 of the GDPR further provide that it would be lawful to retain the personal data if the Company can show that it is necessary:

- **For exercising the right of freedom of expression and information**

- **For compliance with a legal obligation**
- **For the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller**
- **On the grounds of public interest in the area of public health**
- **For archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims**

Right to Data portability

Overview

The right to data portability gives individuals the right to receive personal data they have provided to a controller in a structured, commonly used and machine readable format. It also gives them the right to request that a controller transmits this data directly to another controller.

It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

The right only applies to information an individual has provided to a controller. So, if any personal information is collected from other sources, this does not need to be included in data portability.

The right to data portability entitles an individual to:

- **receive a copy of their personal data; and/or**
- **have their personal data transmitted from one controller to another controller.**

When does the right apply?

The right to data portability only applies when:

- **your lawful basis for processing this information is consent or for the performance of a contract; and**
- **you are carrying out the processing by automated means (i.e. excluding paper files).**

Handling request for Data Portability

Once a request for data portability is received, the company has to act on it at the earliest and latest within a month. The company should provide the personal data in a format that is:

- **structured;**
- **commonly used; and**
- **machine-readable.**

If the company receives a data portability request for transfer of data to another Controller, then it should do so, if feasible. If not, the company shall notify the individual.

General Rules & Guidelines

Data Protection Policy covers the general rules & guidelines for responding to requests from data subjects (as per Article 12), including 1) Form of communication, 2) Timelines and 3) Refusing to act on requests

Action List for Data Subject Request

Refer to separate "Action List for DSAR" to learn more about actions to be taken and timelines for each request type.

Response Templates

Refer to separate "Response Template - All" to learn more about what to include in responses / communications relating to the requests.

Data Subject Request Log

Use the "Data Subject Request Log/Register" to track all data subject requests as evidence of request received, actioned and responded with proper timelines. This is required for regulatory purposes as well.

Annexure 1 - Privacy notice Checklist
What to provide
We provide individuals with all the following privacy information:

- The name and contact details of our organisation.
- The name and contact details of our representative (if applicable).
- The contact details of our data protection officer (if applicable).
- The purposes of the processing.
- The lawful basis for the processing.
- The legitimate interests for the processing (if applicable).
- The categories of personal data obtained (if the personal data is not obtained from the individual it relates to).
- The recipients or categories of recipients of the personal data.
- The details of transfers of the personal data to any third countries or international organisations (if applicable).
- The retention periods for the personal data.
- The rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

When to provide it
We provide individuals with privacy information at the time we collect their personal data from them.
If we obtain personal data from a source other than the individual it relates to, we provide them with privacy information:

- within a reasonable of period of obtaining the personal data and no later than one month;
- if we plan to communicate with the individual, at the latest, when the first communication takes place; or
- if we plan to disclose the data to someone else, at the latest, when the data is disclosed.

How to provide it
We provide the information in a way that is:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- uses clear and plain language.

Changes to the information
We regularly review and, where necessary, update our privacy information.
If we plan to use personal data for a new purpose, we update our privacy information and communicate the changes to individuals before starting any new processing.

Best practice - drafting the information
We undertake an information audit to find out what personal data we hold and what we do with it. We put ourselves in the position of the people we're collecting information about.
We carry out user testing to evaluate how effective our privacy information is.

Best practice - delivering the information
When providing our privacy information to individuals, we use a combination of appropriate techniques, such as:

- a layered approach;
- dashboards;
- just-in-time notices;
- icons; and
- mobile and smart device functionalities.

NOTE – Next review cycle for this policy is March 2027. Management can review policy any time and can make changes depending on the situation.

- All documents related to policies and procedures – any reference to Actionable Science is as good as Rezolve.ai.