

# Cross-border processing or transfers of personal data

Version 8



## Document Information

<b>Name of the document</b>	Cross-border processing or transfers of personal data
<b>Release date</b>	19-Dec-2018
<b>Owned by</b>	Boopathi
<b>Governed by</b>	Mr.Udaya Bhaskar Reddy

## RevisionHistory

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	16-Sep-2024	UpdatedDocumentInformation
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

### [1PURPOSEANDSCOPE4](#)

[Referenceddocuments4](#)

### [BACKGROUND4](#)

### [2CROSS-BORDERPROCESSING4](#)

### [3TRANSFERS OF PERSONALDATA5](#)

[TransferswithintheEU5](#)

[TransfersoutsidetheEU5](#)

[Transfers on the basis of anAdequacyDecision 5](#)

[TransferssubjecttoAppropriateSafeguards6](#)

[Exceptionstothe prohibitionon TransfersoutsidetheEU6](#)

[Infrequent/Limited Transfers7](#)

### [4OtherprovisionsrelatingtoTransfersofPersonalData7](#)

[RighttoInformation&Access7](#)

## 1. Purpose and Scope

Rezolve.ai (the "Company") is committed to complying with applicable laws and regulations related to personal data protection in countries where it operates.

This Policy sets forth the principles relating to cross-border processing and transfers of personal data by the Company.

This Policy applies to:

- Rezolve.ai and its directly or indirectly controlled wholly owned subsidiaries;
- Operations within the European Union (EU), or where the personal data of EU data subjects is processed, irrespective of the processing location.

## 2. Reference Documents

- **European Union (EU) General Data Protection Regulation (GDPR) – Regulation (EU) 2016/679**  
This regulation governs the processing of personal data wholly or partly by automated means, and non-automated processing where the data forms part of a structured filing system.

## 3. Background

Cross-border transfers of personal data outside the EU may increase the risk of misuse or unauthorized access, and may also limit the ability of supervisory authorities to enforce data protection laws.

To mitigate these risks, the GDPR imposes strict conditions on such transfers to ensure that the level of protection provided to individuals is not undermined.

**Non-compliance** may result in significant penalties, including fines up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding year—whichever is higher.

## 4. Rezolve.ai EU Data Policy

All personal data of EU customers is hosted and processed in the **Azure Ireland region**, a member state of the EU. Rezolve.ai acts as a **Processor**, while customers are **Controllers**. No cross-border data transfer occurs outside the EU for EU customers under standard operations.

## 5. Cross-Border Processing (Article 4(23) GDPR)

Defined as:

- Processing by a Controller/Processor with establishments in more than one EU Member State; or
- Processing by a Controller/Processor with a single establishment that substantially affects data subjects in more than one EU Member State.

This concept determines the **Lead Supervisory Authority** when coordinating regulatory oversight.

## 6. Transfers of Personal Data

### 6.1 Within the EU

- The GDPR guarantees **free movement of personal data within the EU** without restriction.

### 6.2 Outside the EU

- Transfers outside the EU (to third countries or international organizations) are permitted **only if**:
  - An adequacy decision is in place, **or**
  - Appropriate safeguards are provided, **or**
  - A specific **derogation** applies under Article 49.

## 7. Transfers Based on Adequacy Decisions (Article 45)

The **European Commission** may determine that certain countries provide an adequate level of protection. Transfers to these countries do **not require further authorization**.

Current “safe” destinations include:

1. Andorra
2. Argentina
3. Canada\*
4. Faroe Islands
5. Guernsey
6. Israel
7. Isle of Man
8. Jersey
9. New Zealand
10. Switzerland
11. Uruguay
12. United States\*\* (*Privacy Shield framework only*)

\* Canada: Commercial organizations only

\*\* United States: Subject to specific frameworks

## 8. Transfers Subject to Appropriate Safeguards (Article 46)

Permitted if **appropriate safeguards** are implemented, such as:

- Standard Contractual Clauses (SCCs)
- Binding Corporate Rules (BCRs)
- Approved Codes of Conduct
- Approved Certification Mechanisms
- Contractual clauses approved by supervisory authorities

These transfers **do not require separate authorization**.

## 9. Exceptions (Derogations – Article 49)

Permissible without adequacy or safeguards **only if** one of the following applies:

- **Explicit consent** from the individual (after being informed of risks)
- **Necessary for contract** with or in the interest of the individual
- Other specific situations (e.g., public interest, legal claims)

These should only be used when no other legal basis applies.

## 10. Infrequent / Limited Transfers

Even without adequacy or safeguards, a transfer may occur if it:

- Involves a **limited number** of individuals
- Is **not repetitive**
- Is **necessary** for compelling legitimate interests of the Company (not overridden by the interests of the data subject)
- Is supported by **documented safeguards** in the Record of Processing Activities

**Company obligations** in such cases:

- Notify the data subject and the relevant supervisory authority
- Assess and document the nature, purpose, risks, and safeguards

Such transfers must remain **exceptional and residual**.

## 11. Other Provisions

### 11.1 Right to Information & Access

Data subjects must be informed if:

- Their data is being transferred outside the EU
- Adequacy decisions or safeguards are in place
- They may obtain a copy of safeguards

### 11.2 Processor Obligations

Processors must:

- Follow documented instructions from the Controller
- Notify the Controller of any legal requirement to transfer data
- Maintain records of processing and transfers (including safeguards and third countries)

## 12. Future Developments

The Company will monitor and may adopt:

- **Codes of Conduct** (Article 40)
- **Certification mechanisms** (Article 42)

These may be issued by industry associations or supervisory authorities to support GDPR compliance.

#### Policy Review

- **Next review cycle:** March 2026
- Management reserves the right to review and modify this policy at any time as needed.

**Note:** Any reference to **Actionable Science** in this or related documents shall be considered equivalent to **Rezolve.ai**.