Rezolv AI Technology Solutions Pvt Ltd
D 214, Kanakia Zillion, LBS Marg, Kurla West, Mumbai 400070.
https://getrezolv.com

PRIVACY POLICY

Version History

Current Version	1.4
Released on	29th July 2026
Classification	Internal Use

Version	Date of Release	Description of Change	Prepared By	Reviewed by	Approved By
1.0	19 Nov 2024	First Release	Information Security Team	Karan Mehta	Board Members
1.2	28 Jan 2025	Policy Update	Information Security Team	Karan Mehta	Board Members
1.3	29 Jan 2026	Annual Review	Information Security Team	Karan Mehta	Board Members
1.4	15 May 2026	Repositioning of Rezolv as Data Processor; alignment with SPDI Rules and DPDP Act 2023; express consent mechanism, biometric consent and erasure, data hosting, cross-border	Information Security Team	Karan Mehta	Board Members

		and AI disclosures; data principal rights			
1.5	29 July 2026	Revision of the Policy	Information Security Team	Karan Mehta	

Table of Contents

1. Introduction

Rezolv AI Technology Solutions Pvt. Ltd. or referred herein as “Rezolv” ("Company", "we", "our", or "us"), a technology service provider that offers a software platform to regulated entities such as banks and non-banking financial companies (NBFCs) to support their debt collection operations. Rezolv does not act as a debt collection or recovery agency and does not itself pursue debts; the regulated entities that engage Rezolv determine the purpose, means, and strategy of any debt collection activity carried out using the Platform, is committed to protecting the privacy of individuals ("you", "your", or "users") who visit our website and/or use our mobile application (collectively, the "Platform"). This Privacy Policy outlines how we collect, use, disclose, and safeguard your personal information when you interact with our Platform.

By accessing or using our Platform, you agree to the collection and use of information in accordance with this Privacy Policy. This policy has been developed in compliance with applicable data protection laws in India, including but not limited to the Information Technology Act, 2000, and the associated Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The purpose of this Privacy Policy is to inform you about the types of personal data we collect, how we process it, your rights concerning your personal data, and the steps we take to protect it. If you do not agree with the terms of this policy, you are advised not to use our Platform.

2. Definitions

For the purposes of this Privacy Policy, the following terms shall have the meanings ascribed to them unless the context requires otherwise:

- **"Personal Data"** refers to any information that relates to an identified or identifiable individual, such as name, contact details, identification number, location data, financial information, or any other data that, either directly or indirectly, can be used to identify a person.
- **"Processing"** means any operation or set of operations performed on Personal Data, whether by automated means or otherwise, including but not limited to collection,

recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction of such data.

- **"Third Parties"** refers to any external entities, including service providers, partners, or affiliates, that may access or process Personal Data in connection with the services provided by Rezolv.
- **"Cookies"** refers to small data files stored on your device when you visit a website, which may be used to remember your preferences, collect analytics, and improve your experience on the Platform.
- **"Data Principal"** refers to the individual to whom the Personal Data relates. In this Privacy Policy, the Data Principal is referred to as "you" or "your."
- **"Data Fiduciary"** means any person, including the State, a company, or any entity, who determines the purpose and means of processing Personal Data. For the purposes of this Privacy Policy, the regulated entities (such as banks and NBFCs) that engage Rezolv's services are the Data Fiduciaries in respect of customer data shared with Rezolv, as they determine the purpose, means, and strategy of processing such data, including any debt collection activity. Rezolv acts as a Data Processor on their behalf. Rezolv may also act as a Data Fiduciary only in respect of limited categories of data it independently collects, such as data of visitors to its website or its own personnel and authorised platform users.
- **"Data Processor"** refers to any person or entity that processes Personal Data on behalf of the Data Fiduciary.
- **"Sensitive Personal Data or Information" (SPDI)** refers to specific categories of personal data that are given a higher level of protection under Indian law. This includes but is not limited to passwords, financial information (such as bank account or payment instrument details), health information, biometric data, sexual orientation, and any other information as prescribed under applicable laws.
- **"Anonymization"** refers to the irreversible process of transforming personal data in such a manner that individuals can no longer be identified, either directly or indirectly, from the data, thereby making it impossible to trace the data back to a specific individual.
- **"Pseudonymization"** refers to the processing of Personal Data in such a manner that it can no longer be attributed to a specific Data Principal without the use of additional information, provided that such additional information is kept separately and is

subject to technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable person.

- **"Data Breach"** refers to any unlawful or unauthorized access, acquisition, disclosure, alteration, loss, or destruction of Personal Data, which compromises the security, confidentiality, or integrity of such data.
- **"Grievance Officer"** refers to the individual designated by the Company, in compliance with Indian laws, who is responsible for addressing any concerns or complaints regarding the processing of Personal Data.
- **"Third-Party Service Providers"** refers to external entities that assist the Company in providing services, including but not limited to IT service providers, cloud service providers, payment processors, or marketing platforms, who may have access to Personal Data for the purpose of performing their services.
- **"User Account"** refers to the account created by a user on the Platform to access services, wherein certain personal information may be collected and stored for providing tailored services.
- **"Withdrawal of Consent"** refers to the right of a Data Principal to revoke their consent to the processing of their Personal Data at any time, without affecting the legality of processing based on consent prior to its withdrawal.

3. Types of Information Collected

Rezolv may collect the following types of information when you use our website and/or mobile application ("Platform"):

3.1 Personal Information

Personal Information refers to any data that can identify you as an individual. The types of Personal Information we collect may include, but are not limited to:

- **Contact Information**: Name, email address, phone number, postal address, and other similar contact details.
- **Identity Information**: Date of birth, government-issued identification numbers (such as PAN, Aadhaar, or passport numbers), and any other information required for identity verification.
- **Financial Information**: Bank account details, credit or debit card information, loan or debt information, credit history, and other financial data shared with Rezolv by its regulated entity clients (such as banks and NBFCs) to enable the operation of the Platform that

supports their debt collection workflows. Such data is processed by Rezolv strictly on the instructions of, and on behalf of, the relevant regulated entity.

- **Communication Data**: Information collected through your correspondence with us, including details of inquiries, complaints, or feedback submitted to us via the Platform or other communication channels.
- **Account Information**: Usernames, passwords, and any other information you provide when creating an account on the Platform.
- **Transaction Data**: Details of payments, recoveries, or any other transactions you perform using the Platform.

3.2 Non-Personal Information

Non-Personal Information refers to any data that cannot be used to identify you as an individual and may include:

- **Device Information**: Details about the device used to access the Platform, such as hardware model, operating system, unique device identifiers, and mobile network information.
- **Browser and Usage Information**: Type of browser, IP address, Internet Service Provider (ISP), browsing patterns, time zone settings, and Platform usage details (e.g., time spent on the Platform, pages viewed, and navigation paths).
- **Log Data**: Information collected automatically each time you interact with our Platform, including server logs, error reports, and timestamps.
- **Cookies and Similar Technologies**: Data collected through cookies, pixels, web beacons, or other tracking technologies that enhance your browsing experience and help us analyze user behavior.

3.3 Sensitive Personal Data or Information (SPDI)

In compliance with Indian laws, we may also collect Sensitive Personal Data or Information (SPDI), including but not limited to:

- **Financial Information**: Bank account details, payment instrument details, or any other payment-related data.
- **Authentication Data**: Passwords, security questions, and other authentication credentials.
- **Biometric Data**: If required by law or with your explicit consent, we may collect biometric data such as face and fingerprints or facial recognition data for identity verification purposes. Such biometric data is collected strictly on an express, opt-in basis and is

processed subject to the safeguards, consent and retention limits described under "Biometric/Face Data Collection and Retention" in the Data Retention Policy below.

The collection of Sensitive Personal Data or Information is subject to specific legal and security safeguards, and we will only process such data with your consent or as required by applicable laws.

By using our Platform, you consent to the collection of the aforementioned information, which is essential for providing our services effectively and in compliance with legal obligations.

4. Method of Data Collection

Rezolv collects Personal Information and Non-Personal Information through various methods to ensure efficient and effective use of our Platform and the services we provide. These methods include:

4.1 Data Received from Regulated Entity Clients and Authorised Platform Users

Rezolv does not directly collect personal data of customers (borrowers) of regulated entities. Customer data is provided to Rezolv by its regulated entity clients (such as banks and NBFCs), who act as the Data Fiduciaries and decide the scope, manner, and purpose of such collection and processing for their debt collection operations. Data that Rezolv may directly receive from authorised platform users (such as the personnel and field agents of regulated entities who use the Platform) and from website visitors who voluntarily provide it includes, but is not limited to:

Account Registration: Information you provide when creating an account on our Platform, such as your name, contact details, and other identity-related data.

- **Communication and Correspondence**: Information you provide when communicating with us through customer service, submitting inquiries, participating in surveys, or providing feedback.
- **Transaction Data**: Information you provide when making payments, updating account information, or engaging with the Platform in connection with the debt collection workflows operated by our regulated entity clients.
- **Forms and Applications**: Information you provide through forms or applications available on our Platform, including those related to identity verification or debt settlement processes.

4.2 Automated Collection

We automatically collect certain information through technology when you interact with our Platform, including:

- **Cookies**: We use cookies and similar tracking technologies to collect data about your browsing behavior, device settings, preferences, and Platform usage patterns. This information helps us enhance user experience, personalize content, and improve the functionality of our services. You can manage your cookie preferences via browser settings or opt out where applicable.
- **Web Analytics**: We use analytics tools such as Google Analytics to automatically collect and analyze information about your interactions with our Platform. This may include your IP address, browser type, referral pages, time spent on pages, and other usage data. This data is anonymized and aggregated for statistical purposes.
- **Log Files**: Our servers automatically collect log files containing information such as your IP address, browser type, access times, pages viewed, and other diagnostic information that helps us monitor and improve the performance of our Platform.
- **Device Information**: We collect information about the device you use to access our Platform, including the hardware model, operating system version, and unique device identifiers. This data is used to optimize compatibility and improve service delivery.

4.3 Third-Party Sources

We may also collect information from third-party sources, including but not limited to:

- **Service Providers**: Information provided by third-party service providers (such as credit bureaus or payment processors) to assist in providing our services or verifying the accuracy of data shared with us by our regulated entity clients.

  Social media and Publicly Available Information: If you interact with our Platform through third-party social media platforms, we may collect data that you make available via such platforms, subject to their privacy settings and policies.
- **Partners and Affiliates**: We may collect information from our business partners, affiliates, or other trusted entities that share data with us to help us deliver our technology platform to our regulated entity clients and comply with legal requirements.

By using our Platform, you acknowledge and agree to the collection of data through these methods as outlined in this Privacy Policy. Where applicable, we will obtain your explicit consent before collecting certain types of data.

5. Purpose of Data Collection

Rezolv collects and processes Personal and Non-Personal Information for specific, legitimate purposes in connection with the services we offer through our Platform. The purposes for which we collect your data include, but are not limited to, the following:

5.1 For Providing the Technology Platform Supporting Debt Collection by Regulated Entities

We process Personal Data shared with us by our regulated entity clients (such as banks and NBFCs), strictly on their instructions and on their behalf, to operate and maintain the technology platform that supports their debt collection activities. The regulated entities determine the purpose, means, and strategy of any debt collection; Rezolv does not itself decide whom to contact, when to contact them, or what collection approach to adopt. The processing supported by Rezolv may include:

- **Verification of Identity**: Ensuring that the data shared with us by our regulated entity clients is accurate and up-todate, and verifying the identity of authorised platform users for the purposes of supporting the regulated entity's debt collection process on the Platform.
- **Debt Collection Activities**: Providing the Platform that enables our regulated entity clients to carry out their own debt collection activities. The communications, negotiations, and transactional decisions are determined and executed by the regulated entity or its authorised personnel using the Platform; Rezolv does not itself initiate contact with borrowers, negotiate debts, or pursue recoveries. Rezolv's role is limited to operating the technology, processing data on the regulated entity's instructions, and maintaining records of activities conducted on the Platform for the regulated entity.
- **Reporting and Record-Keeping**: Maintaining records of interactions, transactions, and recoveries for future reference, audits, or legal requirements.

5.2 Compliance with Legal Obligations

We may collect and process your data to ensure compliance with applicable laws, regulations, and legal processes, including but not limited to:

- **Regulatory Compliance**: Ensuring that the technology services we provide to our regulated entity clients adhere to relevant legal and regulatory requirements, such as the Information Technology Act, 2000, and any rules or guidelines issued by regulatory authorities.

Responding to Legal Requests: Disclosing or providing access to your data as required by law, court orders, or government authorities, including in connection with law enforcement investigations, regulatory audits, or legal proceedings.

- **Fraud Prevention and Risk Management**: Detecting and preventing fraud, unauthorized transactions, and other illegal activities that may compromise the integrity of our services or data.

5.3 Customer Support

We collect and use your data to provide effective customer support services, including:

- **Responding to Inquiries and Complaints**: Addressing any questions, concerns, or complaints you may have regarding our services, and providing timely responses to resolve issues.
- **User Account Management**: Assisting with the creation, updating, and management of your user account, including password resets, account settings, and other related functions.
- **Assisting with Transactions**: Helping you with payments, refunds, and any other transaction-related support you may require during your use of the Platform.

5.4 Improvement of Services and Website/Application

We process Non-Personal Information and analytics data to continuously improve our services, including:

- **Enhancing User Experience**: Using your feedback and behavioural data to optimize the performance, design, and functionality of our Platform, ensuring a better user experience.
- **Platform Maintenance and Development**: Monitoring usage patterns, diagnosing technical issues, and implementing upgrades to improve the stability, security, and performance of our Platform.
- **Personalized Services**: Using cookies and tracking technologies to tailor content and offers based on your preferences, past interactions, and behavior on the Platform.
- **Research and Analytics**: Analyzing trends, usage data, and feedback to gain insights into user needs, preferences, and satisfaction levels, which helps us improve our services and identify new offerings.

Automated Processing and Artificial Intelligence (AI)

The Platform incorporates automated processing and artificial-intelligence and machine-learning (AI/ML) models. In particular, the Platform uses facial-recognition technology to verify the identity of authorised platform users (such as the field agents of our regulated entity clients) before they access sensitive workflows, and may use automated techniques to support fraud detection, anomaly detection and operational security.

Any AI/ML inference performed on Personal Data or biometric data is carried out on cloud infrastructure located in India, and, in respect of customer data, on the documented instructions of and for the purposes determined by the relevant regulated entity Data Fiduciary. Biometric templates and other Personal Data are not used to train third-party or general-purpose AI models, and are not disclosed to any AI-model provider for any purpose other than performing the specific verification or processing instructed.

Rezolv does not use AI or automated processing to make solely automated decisions that produce legal or similarly significant effects on borrowers. All decisions relating to debt collection - including whom to contact and what action to take - are made by the regulated entity or its authorised personnel, and not by Rezolv or its systems.

Your data is collected and processed for these purposes in compliance with Indian data protection laws, and we will not use your information for any purposes other than those outlined in this Privacy Policy without obtaining your prior consent where required.

6. Legal Basis for Processing Personal Data

Rezolv processes Personal Data in accordance with applicable laws and only when we have a lawful basis for doing so. The legal bases for processing your Personal Data include, but are not limited to, the following:

6.1 Consent of the Data Principal

We process your Personal Data based on your explicit and informed consent in the following circumstances:

- **Marketing and Promotional Activities**: When you agree to receive marketing communications, newsletters, or other promotional content, we process your data based on your consent.
- **Optional Data Processing**: When we collect data that is not strictly necessary for the provision of our services (such as certain types of cookies or analytics data), we seek your consent to process such information.

You may withdraw your consent at any time by contacting us or following the opt-out mechanisms provided in the communication, without affecting the legality of processing based on consent before its withdrawal.

6.2 Performance of a Contract

We process your Personal Data when it is necessary to fulfill our contractual obligations with you. This includes:

- **Provision of the Debt Collection Technology Platform**: Processing Personal Data on behalf of, and under contract with, our regulated entity clients (such as banks and NBFCs) to deliver the technology platform that supports their debt collection operations. Rezolv processes such data strictly as a Data Processor; the regulated entity remains the Data Fiduciary and determines the lawful basis for processing in relation to its customers.
- **User Account Management**: Collecting and processing data for the creation, management, and maintenance of your user account, including authentication and security measures.
- **Transaction Processing**: Using your financial information to process payments, refunds, and related transactions associated with the services we provide.

If you do not provide the necessary data for the performance of a contract, we may be unable to fulfill our contractual obligations.

6.3 Compliance with Legal Obligations

Rezolv may process your Personal Data when it is necessary to comply with our legal obligations under applicable laws and regulations. This includes:

- **Regulatory Compliance**: Ensuring compliance with Indian data protection laws, tax laws, anti-money laundering regulations, and other legal requirements that govern the technology services Rezolv provides to regulated entities in connection with debt collection.
- **Legal Disclosures**: Disclosing data to regulatory authorities, law enforcement agencies, courts, or other governmental entities when required by law, such as in response to subpoenas, court orders, or government investigations.
- **Record Retention**: Retaining data as required by law for auditing, reporting, or other compliance purposes.

6.4 Legitimate Uses and Business Operations

We may process your Personal Data for the following legitimate business purposes recognised under applicable Indian law. These purposes relate to the limited categories of data for which Rezolv acts as a Data Fiduciary, based on the documented instructions of the regulated entity that is the Data Fiduciary:

- **Service Improvement**: Using your data to improve and personalize the services we offer, including enhancing the functionality, security, and performance of our Platform.
- **Fraud Prevention and Security**: Processing data to detect and prevent fraud, unauthorized activities, or security breaches that may compromise our services, data, or users.
- **Legal Defence and Risk Management**: Processing data in connection with potential legal claims, compliance audits, or risk assessments to protect our interests, as well as those of our clients and partners.
- **Business Operations**: Using data for general business operations, including conducting research and analysis to better understand user needs, developing new products, and growing our business.

In all instances, we will ensure that the processing of Personal Data is carried out in a fair, transparent, and lawful manner, in compliance with applicable Indian data protection regulations. If you have any questions about the legal basis for processing your Personal Data, you can contact us for further clarification.

7. Use of Cookies and Tracking Technologies

Rezolv uses cookies and similar tracking technologies to enhance your experience on our website and/or mobile application ("Platform"). This section explains the types of cookies we use, how we use them, and your choices regarding their use.

7.1 Types of Cookies Used

Cookies are small data files that are stored on your device when you visit a website. We use the following types of cookies on our Platform:

- **Functional Cookies**: These cookies are essential for the proper functioning of the Platform. They enable core features such as secure logins, session management, and user preferences. Without these cookies, certain features of the Platform may not work correctly.
- **Analytics Cookies**: These cookies help us understand how users interact with the Platform by collecting information about usage patterns, such as pages visited, time spent on the Platform, and any errors encountered. This information is anonymized and used to improve the functionality and performance of our services. For example, we may use Google Analytics to gather and analyze usage data.
- **Performance Cookies**: These cookies collect information about how the Platform performs, including the speed of page loading and any performance issues. The data collected is used to monitor and improve the Platform's efficiency and user experience.
- **Third-Party Cookies**: In some cases, third-party service providers (such as social media platforms or advertising networks) may place cookies on your device when you interact with certain features of our Platform. These cookies are subject to the privacy policies of the respective third parties.

7.2 How We Use Cookies

We use cookies and tracking technologies for the following purposes:

- To remember your preferences and settings (e.g., language, region) during your visits to the Platform.
- To authenticate users and prevent unauthorized access to secure areas of the Platform.
- To track and analyse usage data, helping us understand how users navigate through the Platform and identify areas for improvement.
- To deliver personalized content and advertisements based on your interests and online behavior.
- To manage and improve the security and performance of our Platform.

8. Data Sharing and Disclosure

Rezolv is committed to safeguarding your Personal Data and ensuring that it is shared only under appropriate circumstances. This section outlines the situations in which we may share or disclose your data, and the safeguards we employ to protect your privacy.

8.1 With Third-Party Service Providers

We may share your Personal Data with trusted third-party service providers who assist us in delivering our services. These third parties include, but are not limited to:

- **Payment Processors**: Entities that handle payment processing, including financial institutions and payment gateways.
- **Technology Providers**: Providers of IT infrastructure, cloud storage, data analytics, and technical support that help us maintain and improve our Platform.
- **Authorised Personnel of Regulated Entity Clients**: In-house staff or third-party agents engaged by our regulated entity clients (such as banks and NBFCs) who are authorised by such clients to access the Platform to carry out the client's debt collection activities. Rezolv does not appoint or instruct these agents and does not itself engage in debt recovery.
- **Verification and Authentication Services**: Providers who assist in identity verification and fraud prevention.

All third-party service providers are contractually obligated to process your data in accordance with applicable data protection laws, and they are prohibited from using your data for purposes other than those agreed upon with Rezolv.

8.2 With Regulatory Authorities

We may disclose your Personal Data to regulatory authorities, government agencies, or law enforcement officials when required by law, including but not limited to:

- **Compliance with Legal Requirements**: We may disclose your data to comply with applicable laws, regulations, or legal processes, such as responding to court orders, subpoenas, or requests from government authorities.
- **Regulatory Reporting**: In cases where we are legally required to report certain activities, such as transactions or activities conducted on the Platform by our regulated entity clients, to government or regulatory bodies.
- **Public Safety and Risk Prevention**: When necessary, we may share your data to protect public safety, prevent fraud, or mitigate security risks.

8.3 In Case of Business Transfers

In the event of a corporate transaction such as a merger, acquisition, restructuring, or sale of assets, your Personal Data may be transferred to the new entity or third parties involved in the transaction. This may occur under the following circumstances:

- **Mergers and Acquisitions**: If Rezolv is acquired by or merges with another company, your data may be transferred to the acquiring entity as part of the business transaction.
- **Asset Transfers**: In the case of the sale, liquidation, or transfer of some or all our assets, your data may be included as part of the transferred assets.
- **Business Reorganization**: If we undergo any form of restructuring, your data may be shared with the relevant entities to ensure continuity of service.

In all such cases, we will ensure that the receiving party agrees to use your Personal Data in a manner consistent with this Privacy Policy.

8.4 For Legal Compliance

We may disclose your Personal Data when we believe it is necessary to comply with legal obligations or to protect our rights, including:

- **Legal defence**: To defend or enforce our legal rights in the event of legal disputes, including disputes relating to the technology services we provide to our regulated entity clients.
- **Fraud and Security Monitoring**: To detect, prevent, or respond to fraud, unauthorized access, or other illegal activities.
- **Protection of Others**: To protect the rights, property, or safety of our users, employees, or the public.

In all cases, we ensure that any data shared or disclosed is done in accordance with applicable data protection laws and only to the extent necessary for the purpose at hand. We also take steps to ensure that any third parties receiving your Personal Data maintain confidentiality and security standards equivalent to those outlined in this Privacy Policy.

Data Hosting, Localisation and Cross-Border Transfers

Data Hosting and Location in India: Personal Data processed through the Platform is hosted and processed on cloud infrastructure located in India (currently Amazon Web Services (AWS), Mumbai region). Rezolv maintains its production systems and primary data storage within India.

Compliance with Localisation Requirements: Where Personal Data includes payment or transaction data governed by directions of the Reserve Bank of India (including the RBI directive on Storage of Payment System Data), such data is stored within India in accordance with those requirements and the instructions of the relevant regulated entity.

.

9. Data Security Measures

Rezolv is committed to ensuring the security and confidentiality of your Personal Data. We implement a variety of technical, administrative, and organizational measures to protect your data from unauthorized access, disclosure, alteration, or destruction. The following outlines our key data security measures:

9.1 Encryption, Firewalls, and Other Security Measures

We employ industry-standard security measures to protect your Personal Data, including:

- **Data Encryption**: We use encryption protocols (such as SSL/TLS) to protect your Personal Data during transmission over the internet. This ensures that sensitive information such as financial data and login credentials are securely transmitted between your device and our Platform.
- **Firewalls**: Our systems are protected by firewalls that help prevent unauthorized access to our networks and servers. Firewalls act as a barrier between trusted internal networks and untrusted external sources, ensuring that only authorized traffic is allowed.
- **Access Controls**: We limit access to Personal Data to authorized personnel who require such access for the performance of their duties. Access controls, such as multi-factor authentication (MFA) and role-based access control (RBAC), are in place to ensure that only authorized individuals can access sensitive data.
- **Data Masking and Anonymization**: Where possible, we use techniques such as data masking or anonymization to further protect sensitive information, especially when handling or storing data that is not required to identify specific individuals.
- **Regular Security Audits and Vulnerability Testing**: We conduct regular security audits, vulnerability assessments, and penetration testing to identify and address any potential security risks or vulnerabilities in our systems and infrastructure.
- **Monitoring and Incident Response**: Our systems are continuously monitored for unusual or unauthorized activity. In the event of a security breach or data incident, we have an incident response plan in place to quickly contain and mitigate any damage.

9.2 ISO 27001 or Other Certifications

Rezolv is dedicated to maintaining a robust information security management system (ISMS) that aligns with industry best practices. As part of this commitment:

- **ISO 27001 Certification**: We are certified under the ISO 27001 standard, which demonstrates our adherence to international best practices for information security management. This certification requires us to implement and maintain rigorous security controls to protect the confidentiality, integrity, and availability of Personal Data.
- **Compliance with Industry Standards**: In addition to ISO 27001, we adhere to other relevant security standards and frameworks applicable to the financial and data processing industries. This includes compliance with regulatory security guidelines set forth by Indian authorities, such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
- **Periodic Security Audits**: Our security practices are regularly audited by external auditors to ensure that we maintain compliance with applicable laws, certifications, and internal policies. These audits help us identify potential areas for improvement and ensure continuous enhancement of our security measures.

By implementing these security measures, we strive to protect your Personal Data from unauthorized access, loss, or misuse. However, please note that no system can be completely secure, and while we take steps to safeguard your data, we cannot guarantee its absolute security. In the event of a data breach, we will notify you as required by applicable laws and take immediate steps to mitigate any potential harm.

10. Data Retention Policy

Rezolv is committed to retaining Personal Data only for as long as necessary to fulfill the purposes for which it was collected, or as required by applicable laws and regulations. This section outlines our data retention practices and the criteria we use to determine how long your data will be stored.

10.1 Duration for Which Personal Data Will Be Retained

- **Service-Related Data**: We retain Personal Data for the duration of our engagement with the relevant regulated entity client, including the period during which we provide the technology platform supporting that client's debt collection operations, and for any post-engagement period reasonably required for transition and exit. Retention of customer data is governed by the instructions of the regulated entity that acts as the Data Fiduciary in respect of such data. Once the relationship has ended or the services have been completed, we may retain such data for a specified period to comply with legal and regulatory obligations, resolve disputes, and enforce agreements.

- **Financial Data**: Personal financial information, including payment and transaction data, is retained for as long as necessary to comply with financial reporting, auditing, and taxation requirements under applicable laws.
- **Communication Data**: We retain records of your communications with us, including emails, phone calls, or other forms of correspondence, for as long as needed to resolve your inquiries, maintain customer support records, and comply with legal obligations.
- **Anonymized or Aggregated Data**: In some cases, we may anonymize your Personal Data so that it can no longer identify you. This anonymized data may be retained indefinitely for analytical purposes, research, or to improve our services.
- **Biometric/Face Data Collection and Retention:** We operate as a data processor on behalf of its institutional customers, such as banks and NBFCs, which control the workspace and determine the business purpose of processing. Face data is collected solely for agent identity verification at the time of access to sensitive field workflows and customer-linked financial operations. This is done to support the subscribing institution's operational security, fraud prevention, and audit trail requirements.

  Face data is retained for the duration of the subscribing institution's active engagement with the Rezolv platform. This period is necessary to maintain a verifiable audit trail for all field operations conducted on the institution's behalf, as required under applicable regulatory guidelines.

  Express consent and withdrawal: Face data is collected only after the authorised platform user (agent) has given express, informed, opt-in consent at the time of enrolment. Providing face data is voluntary; where an agent declines, the subscribing institution is offered an alternative means of identity verification. An agent may withdraw consent at any time, following which the face data is deleted as set out below, subject to any minimum retention required by law.

  Retention and erasure: Face data is retained only for so long as the agent remains active and authorised on the Platform, and in any event is securely deleted or irreversibly anonymised within thirty (30) days of the agent's deactivation or offboarding, or of the termination of the subscribing institution's engagement, whichever is earlier, unless a specific legal or regulatory obligation requires longer retention. Other Sensitive Personal Data or Information, such as passwords and authentication credentials, is stored only in encrypted or hashed form and is securely deleted or anonymised once it is no longer required for the purpose for which it was collected.

10.2 Criteria for Determining Retention Periods

The following criteria are used to determine the retention periods for Personal Data:

- **Legal and Regulatory Requirements**: We are obligated to retain certain types of data to comply with applicable laws, including tax, anti-money laundering (AML), and financial regulations. Data retention periods may vary depending on the jurisdiction and specific regulatory requirements.
- **Contractual Obligations**: Data necessary for the performance of a contract, including service agreements with our regulated entity clients, will be retained for the duration of the contract and as required for post-contractual obligations, such as dispute resolution or contract enforcement.
- **Business Needs**: Personal Data may be retained for as long as necessary to meet our legitimate business interests, such as fraud prevention, maintaining accurate business records, and defending or enforcing legal claims.
- **User Requests**: If you request the deletion or anonymization of your Personal Data, we will assess whether we are required to retain the data by law or for legitimate business purposes. Where no such requirement exists, we will delete or anonymize your data as requested.
- **Data Minimization**: We follow the principle of data minimization, ensuring that we only retain the minimum amount of Personal Data necessary to achieve the purposes outlined in this Privacy Policy.

Once the applicable retention period has expired, we will securely delete, anonymize, or otherwise dispose of your Personal Data in accordance with our data disposal procedures, unless we are required to retain it for legal, regulatory, or business purposes.

11. Changes to the Privacy Policy

Rezolv reserves the right to update or modify this Privacy Policy at any time to reflect changes in our practices, legal requirements, or service offerings.

- **Continued Use of the Platform**: By continuing to use our Platform after any changes to this Privacy Policy become effective, you are deemed to have accepted the revised terms. If you do not agree with the updated policy, you must discontinue your use of the Platform and may contact us for further clarification or assistance.

12. Grievance Redressal Mechanism

We take your privacy and concerns seriously and have implemented a Grievance Redressal Mechanism to address any issues related to the collection, use, or protection of your Personal Data.

Your Rights: Access, Review and Correction

You have rights in respect of your Personal Data under applicable Indian law, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 and the Digital Personal Data Protection Act, 2023. These include:

- **Right to review and correct**: In accordance with Rule 5(6) of the SPDI Rules, you may review the information you have provided and require that any Personal Data or Sensitive Personal Data or Information found to be inaccurate or deficient is corrected or amended.
- **Right of access, correction and erasure**: You may request access to, and the correction, completion, updating or erasure of, your Personal Data.
- **Right to withdraw consent**: Where processing is based on your consent, you may withdraw that consent at any time, without affecting the lawfulness of processing carried out before withdrawal.
- **Right to grievance redressal**: You may raise any concern or complaint with the Grievance Officer as set out below.

The extent to which Rezolv can act on such a request depends on its role in relation to the data concerned. For Personal Data that Rezolv collects and controls directly as a Data Fiduciary (such as data of website visitors, its own personnel and authorised platform users), Rezolv will give effect to your rights directly. For customer (borrower) data, in respect of which Rezolv acts only as a Data Processor, Rezolv will forward your request to, and assist, the relevant regulated entity that is the Data Fiduciary, which is responsible for deciding upon it. To exercise any of these rights, please contact the Grievance Officer using the details below.

- **Grievance Officer**: In compliance with applicable Indian laws, we have appointed a Grievance Officer to handle your concerns and complaints regarding data privacy. Rezolv is not a Significant Data Fiduciary under the Digital Personal Data Protection Act, 2023, and is therefore not required to appoint a Data Protection Officer. The Grievance Officer named below is Rezolv's single designated point of contact for all data protection queries and complaints; for customer (borrower) data, in respect of which Rezolv acts only as a Data Processor, the Grievance Officer will coordinate with the relevant regulated entity that is the Data Fiduciary.

Contact Details of the Grievance Officer:

Grievance Officer: Anil Chatla

Email: anil.chatla@rezolv.com
Phone: 9029693406
Address: Unit #214, D-Wing, Kanakia Zillion, Kurla West, Kurla, Mumbai, Maharashtra 400070

- **Process for Raising Concerns or Complaints**:
    - If you have any concerns or complaints regarding the processing of your Personal Data or believe that your privacy rights have been violated, you may contact the Grievance Officer.
    - You may submit your complaint in writing, via email, or through any other form of communication provided in the contact details above.
    - Upon receiving your complaint, the Grievance Officer will acknowledge receipt and investigate the matter. You will receive a response within a reasonable timeframe, typically no later than 30 days from the receipt of your complaint.
    - If you are not satisfied with the resolution provided by the Grievance Officer, you have the right to escalate the matter to the relevant data protection authorities as applicable under Indian law.

13. Applicable Laws and Jurisdiction

This Privacy Policy is governed by and construed in accordance with the laws of India.

In the event of any disputes arising from or relating to this Privacy Policy, the courts of Mumbai, Maharashtra shall have exclusive jurisdiction, subject to any applicable dispute resolution mechanisms agreed upon by the parties.

By using our Platform, you acknowledge that any legal disputes concerning your data and privacy will be governed by Indian law, and you agree to submit to the jurisdiction of the courts of India for resolution of such matters.