LEGAL

Rentablez Guard Data Processing Agreement

Last updated: Version 1.3 | Effective Date: 27 October 2026

DATA PROCESSOR (SERVICE PROVIDER)

Rentablez Software Pvt. Ltd.

Registered: Delaware, USA · Bangalore, India

Email: sales@rentablez.com

Phone: +91 80507 81122

Website: www.rentablez.com

DATA CONTROLLER (CUSTOMER)

To be filled in by the Customer upon signing.

Preamble — Background and Purpose

This Data Processing Agreement ("DPA" or "Agreement") governs how Rentablez Software Pvt. Ltd. ("Rentablez", "we", "us") processes personal and device data on behalf of the Customer ("you", "your company") in connection with Rentablez Guard, a remote lock and device-tracking service for rented laptops.

Rentablez Guard consists of the Guard web application, the Rentablez Guard agent installed on the Customer's Windows, macOS and Linux (Beta) laptops, desktops and servers, and the Guard features available inside the Rentablez rental management software. Rentablez acts as the Data Processor and the Customer as the Data Controller. Rentablez acts solely on the documented instructions of the Customer and does not process Customer Data for its own purposes.

This DPA forms part of, and supplements, the Customer's subscription to Rentablez Guard and the Rentablez Terms of Service. Where the Customer also uses the Rentablez rental management software, the Rentablez Data Processing Agreement continues to apply to that software, and this DPA applies in addition to it for Guard. In the event of conflict, this DPA shall take precedence on matters of data protection relating to Rentablez Guard.

1. Definitions

For the purpose of this Agreement, the following terms shall have the meanings set out below:

- **"Customer Data"** means all data processed through Rentablez Guard on behalf of the Customer, including Device Telemetry, location data, lock records, staff account data and audit records.
- **"Managed Device"** means a laptop, desktop or server owned or controlled by the Customer on which the Agent has been installed using an activation code issued to the Customer, or which the Customer has paired to its account in Guard using the pairing code the Agent displays.
- **"Agent"** means the Rentablez Guard software installed on a Managed Device.
- **"End User"** means any natural person who holds or uses a Managed Device, including the Customer's own customers who rent the laptop.
- **"Device Telemetry"** means the technical information the Agent reports about a Managed Device, as described in Section 4.
- **"Personal Data"** means any information relating to an identified or identifiable natural person, as defined under applicable Indian and international data protection laws, including India's Digital Personal Data Protection Act, 2023 (DPDP Act). Location data and Device Telemetry linked to a rental become Personal Data of the End User.
- **"Processing"** means any operation performed on Customer Data, including collection, storage, retrieval, use, disclosure, or deletion.
- **"Data Controller"** means the Customer, who determines the purposes and means of Processing Customer Data, including when a Managed Device is locked, unlocked or located.

- **"Data Processor"** means Rentablez, which processes Customer Data on behalf of the Data Controller.
- **"Sub-Processor"** means any third-party service provider engaged by Rentablez that processes Customer Data.
- **"Security Incident" or "Data Breach"** means any unauthorised access, disclosure, loss, or destruction of Customer Data.

2. Rentablez's Core Data Protection Commitment

Rentablez makes the following binding commitments to the Customer regarding Customer Data:

- We will **NEVER** sell your data or your End Users' data to any third party for any reason.
- We will **NEVER** use your data to train AI models or machine learning systems.
- We will **NEVER** share your data with competitors, advertisers, or data brokers.
- We will **NEVER** use your data for our own marketing, analytics, or business intelligence purposes.
- The Agent does **NOT** read documents or files, capture the screen, log keystrokes, or track browsing or application use.
- We will **NEVER** lock, unlock or locate a Managed Device on our own initiative — only on the instruction of the Customer's authorised users.
- We will process your data **ONLY** as per your documented instructions and the scope of the Rentablez Guard service.

3. Scope and Purpose of Data Processing

Rentablez shall process Customer Data solely for the following documented purposes:

- Remotely locking and unlocking Managed Devices on the Customer's instruction, displaying the Customer's lock-screen message, and issuing one-time offline unlock codes.
- Showing the status of each Managed Device (online, offline, locked, lock pending) and the Agent version installed.

- Pairing a Managed Device installed without an activation code to the Customer's account and to one of its units, on the Customer's instruction.
- Passing a request to uninstall the Agent to the Customer, and removing the Agent only once the Customer approves it.
- Sending alerts to the Customer's staff, by email, WhatsApp or both as the Customer chooses, when a hardware change is detected, format protection is lost, precise location is turned off, a Managed Device stays offline longer than the period the Customer sets, or a Linux machine health reading turns critical.
- Detecting hardware changes on a Managed Device against its recorded baseline and alerting the Customer.
- On a Linux Managed Device installed with the health monitor, showing its machine health (disk space, memory, temperature, load and failed system services) and alerting the Customer when a reading is critical.
- On a Linux Managed Device set up as a server, blocking its network traffic, other than the connection to Rentablez, while the Customer has it locked.
- Verifying BIOS anti-theft settings and safekeeping the Customer's BIOS supervisor password on supported laptops (Beta).
- Reporting operating-system format protection status on supported laptops (Beta).
- Showing the approximate location of a Managed Device and, where enabled under Section 5, its precise location.
- Managing the Customer's Guard licences, renewals and payments.
- Providing technical support and resolving issues reported by the Customer, and complying with legal obligations applicable to Rentablez.

Rentablez shall not process Customer Data for any other purpose without explicit written consent from the Customer.

4. Types of Customer Data Processed

In the course of providing Rentablez Guard, Rentablez may process the following categories of data on behalf of the Customer:

- **Device identity and hardware:** asset tag, device hostname, Agent version, and a hardware fingerprint made up of component identifiers and serial numbers (for

example processor, memory, storage, network adapters and motherboard).

- **Device status:** check-in times, online/offline status, lock state, lock and unlock history, offline unlock code use, pairing codes and pairing records, uninstall requests and the Customer's decision on them, and Agent events such as the Agent being stopped.
- **Network and approximate location:** the public IP address a Managed Device connects from, used to work out an approximate, city-level location. The IP address is stored to avoid repeated lookups and is not shown to the Customer's users.
- **Machine health (Linux, optional):** every few minutes, processor and memory use, system load, disk space per mounted filesystem, the highest temperature sensor reading, uptime, the names of failed system services, and the Agent's own connection status. No file names, file contents, process lists or user activity are collected.
- **Precise location (optional):** the Wi-Fi or GPS position of a Managed Device and its accuracy, reported only when the Agent was installed with Precise location switched on, and the derived street address.
- **Security settings:** reported BIOS anti-theft and operating-system format protection status, and the BIOS supervisor password the Customer chooses to store, kept encrypted.
- **Customer account data:** names, email addresses and roles of the Customer's staff users, the organisation email address and WhatsApp or mobile number used to receive alerts, the Customer's alert channel choices, and an audit trail of their actions in Guard.
- **Billing data:** licence counts, invoices and payment status for Guard subscriptions.

Rentablez does not intentionally collect sensitive personal data (such as biometric data, health records, or the contents of a Managed Device) through Rentablez Guard. "Machine health" above describes the condition of the device, not the health of any person.

5. Customer Obligations Specific to Device Management

Because Rentablez Guard acts on devices held by End Users, the Customer, as Data Controller, is responsible for:

- Having a lawful basis to manage, lock and locate each Managed Device, and stating in its rental agreement with the End User that the device is managed and may be remotely locked and located.
- Informing End Users, before a Managed Device is handed over, that the Agent is installed and what data it reports.
- Obtaining the End User's consent before enabling Precise location, and keeping a record of that consent. The Agent installer asks the installer to confirm consent but Rentablez does not record or verify it.
- Using Rentablez Guard only to protect its own assets, and not to monitor any person for any other purpose.
- Limiting access to lock, unlock, location and BIOS password features to authorised staff, and keeping their login credentials secure.

6. Security Measures

Rentablez implements appropriate technical and organisational security measures to protect Customer Data, including but not limited to:

- Encryption of data in transit using TLS (Transport Layer Security).
- Encryption of data at rest on cloud infrastructure.
- A unique key for each Managed Device, with every request from the Agent signed so that one device cannot report for, or receive commands meant for, another.
- Separation of each Customer's data so that it is visible only to that Customer's users.
- Stored BIOS supervisor passwords encrypted with a dedicated key (AES-256-GCM) and revealable only by the Customer's administrators.
- An audit trail of lock, unlock, password reveal, pairing, uninstall requests and their approval or rejection, record removal and other device actions, recording who performed each one.
- Role-based access controls ensuring only authorised Rentablez personnel can access Customer Data, and only when necessary.

- Secure hosting on reputable cloud infrastructure with automated backups, and employee confidentiality obligations covering all Rentablez staff.

7. Sub-Processors

Rentablez may engage the following categories of trusted sub-processors to deliver Rentablez Guard. All sub-processors are bound by data protection obligations no less stringent than this Agreement:

- **Cloud hosting providers** — for infrastructure, storage and backups.
- **Email and WhatsApp delivery services** — solely for sending alerts to the Customer's staff, such as hardware change, format protection, offline, location-off and machine health alerts. WhatsApp alerts are sent only when the Customer turns them on, and only to the Customer's own number; no End User contact details are shared.
- **Payment gateway providers** (Stripe, Razorpay) — solely for processing the Customer's Guard subscription payments.
- **Map and reverse-geocoding providers** (Ola Maps in India, OpenStreetMap elsewhere) — solely to turn a precise location into a street address and to display maps. Only coordinates are sent; no device or End User identity is shared.

Approximate location is worked out from the IP address using a geolocation database hosted by Rentablez itself. IP addresses are not sent to a third party for this purpose.

Rentablez will notify the Customer of any significant change in sub-processors that may affect the security of Customer Data, providing a minimum of 30 days' notice where possible.

8. Data Retention and Deletion

Rentablez retains Customer Data only for as long as needed to provide Rentablez Guard and as required by applicable law:

- Location history is deleted automatically after **90 days**.

- Machine health history is deleted automatically after **30 days**. Only the latest report is kept beyond that.
- The Customer may at any time delete the Agent, hardware, location, BIOS, format protection and machine health records of any Managed Device from within Guard. The audit record that the deletion took place is kept.
- Uninstalling the Agent stops all further reporting from that Managed Device.

Upon termination or expiry of the Customer's Guard subscription:

- The Customer may export its data within **30 days** of account closure.
- Rentablez shall delete all Customer Data from its active systems within **60 days** of subscription termination.
- Backup copies of Customer Data (held for disaster recovery purposes) shall be purged within **90 days** of subscription termination.
- Rentablez shall provide written confirmation of deletion upon request.

Data may be retained beyond these periods only if required by Indian law or a lawful order from a competent authority.

9. Data Breach Notification

In the event Rentablez becomes aware of a confirmed Security Incident affecting Customer Data, Rentablez shall:

- Notify the Customer without undue delay, and in any event within **72 hours** of becoming aware of the incident.
- Provide the Customer with details of the nature of the breach, data categories affected, likely consequences, and remedial measures taken.
- Cooperate fully with the Customer in investigating and managing the incident, including any notice the Customer must give to End Users.
- Take immediate steps to contain, mitigate, and remediate the breach.

10. Customer Rights and End User Requests

The Customer, as Data Controller, retains the following rights:

- Right to issue documented instructions to Rentablez regarding the Processing of Customer Data.
- Right to audit Rentablez's data processing practices upon reasonable notice (annually or following a Security Incident).
- Right to request deletion, correction, or export of Customer Data at any time.
- Right to object to any Processing activity not covered by this Agreement.

End Users exercise their rights through the Customer. If Rentablez receives a request directly from an End User, it will pass the request to the Customer without undue delay and will help the Customer respond, including by locating or deleting that End User's data.

11. Legal Compliance

Rentablez processes Customer Data in compliance with applicable data protection laws, including:

- India's Digital Personal Data Protection Act, 2023 (DPDP Act).
- Information Technology Act, 2000 and the IT (Amendment) Act, 2008.
- Any other applicable local or sectoral data protection regulations.

Where Customer Data includes personal data of individuals located in other jurisdictions (e.g., EU citizens under GDPR), Rentablez shall cooperate with the Customer to implement appropriate safeguards for such cross-border transfers.

12. Confidentiality

Rentablez shall treat all Customer Data as strictly confidential. Rentablez shall ensure that:

- Only authorised personnel who need access to Customer Data for the purpose of delivering the service are granted such access.
- All Rentablez employees and contractors with access to Customer Data are bound by written confidentiality obligations.

- Customer Data shall not be disclosed to any third party except as expressly permitted under this Agreement or required by law.

13. Limitation of Liability

Rentablez's total liability to the Customer under this Agreement for any data protection breach shall not exceed the total fees paid by the Customer to Rentablez for Rentablez Guard in the twelve (12) months preceding the event giving rise to the claim, unless the breach is a result of Rentablez's gross negligence or willful misconduct.

Rentablez shall not be liable for breaches arising from the Customer's failure to maintain adequate security of their own account credentials or systems, for lock, unlock or location actions taken by the Customer's users, or for the Customer's failure to meet its obligations under Section 5.

14. Governing Law and Disputes

This Agreement shall be governed by the laws of India. Any dispute arising out of or in connection with this Agreement shall first be attempted to be resolved amicably between the parties.

If not resolved within 30 days of written notice, disputes shall be subject to the exclusive jurisdiction of the courts of Bangalore, Karnataka, India.

15. Amendments

Rentablez may update this Agreement periodically to reflect changes in law, technology, the data Rentablez Guard collects, or business practices. The Customer will be notified of material changes at least 30 days in advance via email or in-app notification.

Continued use of Rentablez Guard after the effective date of any amendments constitutes acceptance of the revised Agreement.

Questions about this agreement?

Contact us at sales@rentablez.com or call +91 80507 81122