

PRIVACY POLICY

Please Read Before Proceeding: By clicking “I Agree”, checking the consent box on this page, or otherwise providing a clear affirmative action on the Platform or in any Equipp-hosted form, you acknowledge that you have read and understood this Privacy Policy and consent to the processing of your personal data as described herein and as contemplated under the Master Terms and Conditions and any applicable Addendum (together, the “Customer Agreements”). If you do not consent, do not proceed with registration or use of the Platform.

TABLE OF CONTENTS

1.	REGULATORY FRAMEWORK AND ROLE.....	2
2.	SCOPE AND RELATIONSHIP WITH CUSTOMER AGREEMENTS.....	2
3.	PERSONAL DATA COLLECTED.....	2
4.	LEGAL BASES AND PURPOSES OF PROCESSING.....	4
5.	MDM, DEVICE DATA AND CUSTOMER RESPONSIBILITIES.....	5
6.	DATA SHARING AND TRANSFERS.....	5
7.	DATA SECURITY AND RETENTION.....	6
8.	COOKIES AND TRACKING TECHNOLOGIES.....	7
9.	DATA PRINCIPAL RIGHTS AND GRIEVANCE REDRESSAL.....	7
10.	THIRD-PARTY LINKS AND FORMS.....	8
11.	CHILDREN’S DATA.....	8
12.	DATA BREACH NOTIFICATION.....	8
13.	UPDATES TO THIS PRIVACY POLICY.....	9

1. REGULATORY FRAMEWORK AND ROLE

- 1.1 Equipp processes “digital personal data” in its capacity as a Data Fiduciary under the Digital Personal Data Protection Act, 2023 (“DPDP Act”) and the Digital Personal Data Protection Rules, 2025 (“DPDP Rules”), as amended or re-enacted from time to time. All personal data collected and processed by Equipp is handled in accordance with the purposes, legal bases, and safeguards set out in this Privacy Policy.
- 1.2 Equipp also complies with the applicable provisions of the Information Technology Act, 2000, including the obligations on reasonable security practices and procedures, and the obligations applicable to intermediaries and e-commerce entities under rules made thereunder.
- 1.3 The Platform is operated as an e-commerce entity and Equipp discharges its obligations as such, including under the Consumer Protection (E-Commerce) Rules, 2020, with respect to grievance redressal, display of information, and consumer rights.

2. SCOPE AND RELATIONSHIP WITH CUSTOMER AGREEMENTS

- 2.1 This Privacy Policy applies to all individuals who access or use the Equipp website (equipp.in), mobile application, or any other digital interface operated by Equipp or its Affiliates, including any Jotform or other data-collection forms used for lead capture, onboarding, or KYC purposes (collectively, the “Services”), including:
 - 2.1.1 individual customers using Equipp for personal equipment rentals (“Individual Accounts”);
 - 2.1.2 authorised representatives, authorised signatories, and contact persons of corporate or institutional customers (“Business Accounts”);
 - 2.1.3 personal guarantors and other signatories to any Applicable Addendum executed in connection with a Business Account; and
 - 2.1.4 visitors browsing the Platform or interacting with Equipp-hosted forms, whether or not they proceed to registration or order placement.
- 2.2 This Privacy Policy forms part of the suite of Customer Agreements that governs the relationship between Equipp and its customers. In the event of any inconsistency between this Privacy Policy and the Customer Agreements, the mandatory provisions of applicable law shall prevail, followed by the Customer Agreements, and thereafter this Privacy Policy.

3. PERSONAL DATA COLLECTED

- 3.1 Identity and Contact Data
 - 3.1.1 Name, title, and contact details - Full name, title, designation, email address, mobile number, residential or business address, and any other contact information provided at registration, during KYC, or in the course of any transaction.
 - 3.1.2 Government identifiers - Permanent Account Number (PAN) and PAN-linked mobile number, as required for identity verification and KYC; PAN card image as part of the digital KYC verification flow; and Aadhaar OTP verification or equivalent, where required for Individual Accounts for Monthly Rental Fees exceeding the threshold specified under the Master Terms and Conditions.
 - 3.1.3 Optional professional identifiers - LinkedIn profile URL or similar professional identifier where voluntarily provided by the customer to support credit and risk assessment.
- 3.2 Account, Order and Rental Data
 - 3.2.1 Account data - Account type (Individual or Business), account registration details, KYC and eligibility status, and account history.
 - 3.2.2 Order and rental data - Order history, Rental Periods, descriptions and serial numbers of Equipment rented, delivery and pickup addresses, return status, and asset condition records.

- 3.2.3 Payment and billing data - Monthly Rental Fee amounts, Security Deposit amounts, applicable charges under the Table of Charges (including late payment charges, Cancellation Fees, Handling Fees, and Revenue Loss Charges), refund details, and GST-compliant invoice records, in accordance with Equipp's pricing and billing practices under the Master Terms and Conditions.
- 3.3 KYC and Credit Assessment Data
 - 3.3.1 KYC data - Attributes collected through Equipp's digital KYC verification flow, including PAN details, PAN-linked mobile verification, and related verification responses received from authorised KYC service providers.
 - 3.3.2 Credit assessment data - Soft credit check results obtained via authorised third-party bureau and data providers (including providers such as Decentro and credit information bureaus) based on PAN and PAN-linked mobile number, including bureau responses and scores where applicable. Equipp uses this data solely for the purpose of assessing creditworthiness and managing default risk, as contemplated under the Master Terms and Conditions.
- 3.4 Device and Technical Data
 - 3.4.1 Platform access data - Device identifiers, IP address, browser type and version, operating system, and log data captured when you access the Platform, submit a form, place an order, or accept any of the Customer Agreements. This data may include the date and time of access, the Agreement version accepted, and the Customer's account identifier, and is maintained as a tamper-evident record of acceptance.
 - 3.4.2 Cookies and tracking technologies - Data collected through cookies and similar technologies, as further described in the relevant clause(s) of this Privacy Policy.
- 3.5 MDM and Asset Protection Data
 - 3.5.1 Device monitoring data - Where Equipment delivered under the Customer Agreements has pre-installed mobile device management ("MDM") software, Equipp collects data on device location, hardware status, device health, and asset condition, in accordance with the MDM consent given by the customer under the applicable Addendum. The specific MDM software used, its capabilities, and its data access scope are disclosed in the relevant Order Confirmation.
- 3.6 Communications and Support Data
 - 3.6.1 Authorised Channel communications - Records of orders, instructions, and communications received via email, WhatsApp, SMS, calls, and in-app channels that constitute Authorised Channel communications under the Master Terms and Conditions, together with associated metadata.
 - 3.6.2 Support and grievance records - Support tickets, query records, grievance submissions, and associated metadata including timestamps, channel of submission, handling officer identity, and resolution outcome, maintained in compliance with applicable e-commerce grievance obligations.

4. LEGAL BASES AND PURPOSES OF PROCESSING

- 4.1 Legal Bases under the DPDP Act - Equipp processes personal data on the following grounds recognised under the DPDP Act and DPDP Rules:
 - 4.1.1 Consent - Free, specific, informed, unconditional, and unambiguous consent given through a clear affirmative action, including clickwrap acceptance on the Platform, explicit consent checkboxes in Jotform or other onboarding forms, and express MDM consent under the applicable Addendum. Consent is sought separately for distinct processing purposes where required under the DPDP Act.
 - 4.1.2 Legitimate uses - Processing for lawful purposes where consent is not required under the DPDP Act, including compliance with legal and regulatory obligations, enforcement of

contractual rights and claims, fraud prevention, and any other purpose notified by the Central Government under the DPDP Act, to the extent applicable.

- 4.2 Key Purposes of Processing
 - 4.2.1 Onboarding and KYC - Verifying the identity, eligibility, and account type of customers; conducting KYC verification and re-verification; processing and, where applicable, automatically cancelling unverified orders as contemplated under the Master Terms and Conditions; and maintaining KYC records for the periods required by applicable law.
 - 4.2.2 Credit assessment and risk management - Conducting soft credit checks using PAN, PAN-linked mobile number, and other permissible parameters via authorised third-party data and bureau providers, to assess creditworthiness and manage default risk, in accordance with the eligibility and KYC requirements under the Master Terms and Conditions.
 - 4.2.3 Order processing, delivery, and returns - Managing orders from placement to completion; scheduling and coordinating delivery and pickup through logistics partners; tracking Equipment assets throughout the Rental Period; and handling Equipment returns and asset condition assessments as required under the Master Terms and Conditions.
 - 4.2.4 Payments, billing, and collections - Facilitating payments through payment gateways; issuing GST-compliant invoices and billing records; applying charges per the Table of Charges incorporated into the Master Terms and Conditions; and managing refunds, collections, and recovery of amounts due.
 - 4.2.5 MDM and asset protection - Monitoring location, hardware status, and device health of MDM-enabled Equipment; and, in circumstances defined under the applicable Addendum and the Master Terms and Conditions, issuing remote lock or remote wipe commands solely for the purpose of asset protection and recovery. MDM data is used exclusively for asset protection and is not used for any other purpose.
 - 4.2.6 Customer support and grievance redressal - Responding to queries, complaints, and grievances; operating mandated grievance mechanisms; maintaining records of resolutions; and complying with acknowledgment and response timelines prescribed under applicable e-commerce and consumer protection rules.
 - 4.2.7 Analytics and service improvement - Analysing usage patterns, platform performance metrics, and aggregated data to improve the Platform, user experience, pricing models, and operational workflows. Where feasible, Equipp uses anonymisation or pseudonymisation in connection with analytics activities.
 - 4.2.8 Legal and compliance - Maintaining clickwrap acceptance logs and key contractual records for the periods required under applicable law and limitation periods; responding to lawful requests from governmental authorities, regulators, and courts; enforcing Equipp's contractual rights; and detecting, preventing, and addressing fraud, misuse, and unlawful activity.

5. **MDM, DEVICE DATA AND CUSTOMER RESPONSIBILITIES**

- 5.1 Under the applicable Addendum, Business Account customers and, where applicable, personal guarantors, expressly consent to Equipp's use of MDM functions on Equipment, including monitoring of location, hardware status, and device health, and the issuance of remote lock or remote wipe commands in the circumstances described in the Master Terms and Conditions. Equipp commits to process device data in accordance with the DPDP Act and to use such data solely for asset protection purposes. Device data is not shared with third parties except as required by applicable law.
- 5.2 The Customer is solely responsible for all personal data and business data stored on Equipment during the Rental Period. The Customer must perform a factory reset or equivalent data deletion

equipp*by Equipp Synergy Pvt. Ltd.*

process on Equipment before returning it to Equipp. Equipp performs a secondary wipe as a matter of practice but is not obliged to provide data recovery services and is not liable for loss of data arising from Equipment return, Equipment swap, or a lawful remote wipe under the Master Terms and Conditions, except in cases of wilful misconduct or gross negligence by Equipp.

- 5.3 The Customer acknowledges that Equipment delivered under the Addendum may have MDM software pre-installed. The specific MDM software used, its capabilities, and its data access scope will be disclosed in the relevant Order Confirmation issued by Equipp.

6. DATA SHARING AND TRANSFERS

- 6.1 Equipp may share personal data with the following categories of recipients, in each case only to the extent necessary for the purposes described in this Privacy Policy and under appropriate contractual and legal safeguards:
- 6.1.1 Service providers and data processors - KYC and identity verification providers; credit information bureaus and data providers (including providers such as Decentro); payment gateway operators; logistics and delivery partners; MDM software vendors; analytics and technology providers; cloud infrastructure and hosting providers; and other third parties engaged to support Equipp's operations. All such service providers are engaged under contractual arrangements that require them to process personal data only on Equipp's instructions and for the purposes for which it was shared.
 - 6.1.2 Group entities and permitted assigns - Equipp's Affiliates (as defined in the Master Terms and Conditions) and permitted successors and assigns, to the extent permitted under the Customer Agreements and in accordance with applicable Indian contract law.
 - 6.1.3 Regulators, authorities, and law enforcement - Central and state government authorities, courts, tribunals, regulatory bodies, and law enforcement agencies, where disclosure is required by applicable law, court order, or regulatory direction, or where Equipp reasonably determines that disclosure is necessary to protect its legal rights, assets, customers, or users.
- 6.2 Any processing of personal data outside India will be undertaken in accordance with Section 16 of the DPDP Act and any notifications issued by the Central Government restricting or conditioning data transfers to specified jurisdictions. Equipp will not transfer personal data to any jurisdiction that has been restricted or blacklisted under applicable Government notification.

7. DATA SECURITY AND RETENTION

- 7.1 Security Measures
- 7.1.1 Equipp implements reasonable security practices and procedures, including technical and organisational safeguards designed to protect personal data against unauthorised access, alteration, disclosure, and destruction, in accordance with the obligations under the DPDP Act, the DPDP Rules, and the standard of "reasonable security practices" under the Information Technology Act, 2000.
 - 7.1.2 Equipp's security measures include, without limitation, access controls restricting personal data access to authorised personnel; logging and monitoring of access to personal data systems; encryption and pseudonymisation where technically appropriate; and backup and business continuity measures for critical customer data.
 - 7.1.3 Notwithstanding Equipp's security measures, no internet or electronic storage system is entirely secure. Equipp cannot guarantee absolute security of personal data transmitted to or stored on the Platform. The Customer is responsible for maintaining the security of its account credentials and Authorised Channel details.
- 7.2 Retention Periods
- 7.2.1 Equipp retains personal data only for as long as necessary to fulfil the purposes described in this Privacy Policy, or as required by applicable law and limitation periods, including the following minimum periods:

- (a) Clickwrap acceptance records - Clickwrap acceptance logs, Agreement versions accepted, and associated metadata: for a minimum of five (5) years from the date of acceptance, or such longer period as may be required under applicable law or limitation periods applicable to contract enforcement.
- (b) KYC and credit assessment records - For the periods mandated by applicable data protection law, financial sector norms, and Equipp's internal risk and compliance policies, which may extend beyond the term of the Master Relationship.
- (c) Order, rental, billing, and tax records - For a minimum of seven (7) years from the date of the relevant transaction, as required by applicable tax and commercial record-keeping obligations.
- (d) Support and grievance records - For the period required under applicable e-commerce, consumer protection, and data protection laws, and for the duration of any associated dispute or legal proceeding.
- (e) MDM and device monitoring data - For the duration of the relevant Rental Period and such additional period as is reasonably necessary for asset protection, dispute resolution, or compliance purposes.

7.3 Upon expiry of the applicable retention period, personal data that is no longer required for any lawful purpose is deleted or irreversibly anonymised, consistent with Equipp's obligations on erasure under the DPDP Act.

8. COOKIES AND TRACKING TECHNOLOGIES

8.1 The Platform uses cookies and similar technologies, including web beacons, pixels, and local storage, to operate the website and mobile application, maintain user sessions, remember preferences, conduct analytics, and detect fraud or misuse, in accordance with applicable Indian data protection practice.

8.2 Cookies used on the Platform may include the following categories:

- 8.2.1 Strictly necessary cookies - Required for the Platform to function and cannot be disabled. These include session management cookies, authentication tokens, and security cookies.
- 8.2.2 Performance and analytics cookies - Used to collect information about how visitors use the Platform, including pages visited, errors encountered, and navigation paths, in order to improve the Platform and user experience. Data collected through these cookies may be aggregated and anonymised.
- 8.2.3 Preference cookies - Used to remember user settings and preferences, such as language preferences and display choices, to provide a more personalised experience.

8.3 You may manage cookie preferences through your browser settings. However, disabling certain categories of cookies may affect the functionality of the Platform, including the ability to place orders, complete KYC, or access account features. Equipp will provide a cookie consent mechanism on the Platform in accordance with applicable data protection requirements.

9. DATA PRINCIPAL RIGHTS AND GRIEVANCE REDRESSAL

9.1 Rights of Data Principals

9.1.1 Under the DPDP Act and DPDP Rules, data principals have the following rights in respect of personal data processed by Equipp:

- (a) Right to access information - To obtain a summary of the personal data being processed by Equipp and the purposes for which it is being processed.
- (b) Right to correction and erasure - To correct inaccurate or incomplete personal data held by Equipp; and to request erasure of personal data that is no longer necessary for the purposes for which it was collected, subject to Equipp's legal obligations and legitimate interests in retaining such data.

equipp*by Equipp Synergy Pvt. Ltd.*

- (c) Right to grievance redressal - To lodge a complaint or grievance with Equipp and receive a response within the timelines prescribed under applicable law; and, if dissatisfied with Equipp's response, to escalate the matter to the Data Protection Board of India in accordance with the DPDP Act.
- (d) Right to withdraw consent - To withdraw consent to the processing of personal data at any time by written notice to Equipp. Withdrawal of consent does not affect the lawfulness of processing undertaken on the basis of consent prior to its withdrawal. Withdrawal of consent may affect the Customer's ability to use certain features of the Platform or to continue the Master Relationship, and may constitute grounds for Equipp to take steps permitted under the Customer Agreements.
- (e) Right to nominate - To nominate another individual to exercise rights under the DPDP Act on the data principal's behalf in the event of their death or incapacity, where such nomination mechanism has been operationalised in accordance with the DPDP Act and DPDP Rules.

9.2 Exercising Your Rights

9.2.1 To exercise any of the rights set out in the relevant clause(s) in this Privacy Policy, or to raise privacy-related queries, complaints, or requests, customers may contact Equipp through the following channels:

- (a) Email: privacy@equipp.in
- (b) Post: Equipp Synergy Pvt. Ltd., [\[Registered Office Address\]](#), Bangalore, India.

9.2.2 Equipp will acknowledge receipt of a data principal request within a reasonable period and will provide a substantive response within the timelines prescribed under applicable law. Equipp will publish the business contact details of its designated privacy contact or Data Protection Officer on the Platform and will update these details as required by the DPDP Rules.

9.3 Grievance Officer and E-Commerce Compliance

9.3.1 Equipp has appointed a Grievance Officer for the Platform. The name, designation, and contact details of the Grievance Officer are published on the Platform and updated as required. Grievances may be submitted through the Platform's designated grievance mechanism or by contacting the Grievance Officer directly.

9.3.2 Equipp will acknowledge grievance submissions within 48 (forty-eight) hours of receipt and will resolve them within the timelines prescribed under applicable e-commerce and consumer protection rules, including the Consumer Protection (E-Commerce) Rules, 2020.

10. THIRD-PARTY LINKS AND FORMS

10.1 The Platform may contain links to external websites or embed third-party forms and data-collection interfaces, including Jotform or similar tools, for the purpose of collecting customer information in connection with lead capture, onboarding, or KYC workflows. Equipp does not control the privacy practices of third-party websites and is not responsible for their content or privacy policies.

10.2 Where third-party forms are used as part of Equipp's onboarding or data-collection workflows, Equipp will ensure that this Privacy Policy is hyperlinked and accessible at the point of data collection, and that a mandatory consent checkbox is included before submission. Backend logging of the timestamp, version of the Privacy Policy accepted, and relevant metadata will be maintained to evidence valid consent.

11. CHILDREN'S DATA

11.1 Equipp's Services are intended only for individuals who have attained the legal capacity to contract under applicable Indian law and are not designed for children as defined under the

DPDP Act. Equipp does not knowingly collect or process personal data of children in connection with its standard platform operations.

- 11.2 If Equipp becomes aware that personal data of a child has been collected contrary to the requirements of the DPDP Act, it will take prompt steps to delete such data and, where required, notify the Data Protection Board of India in accordance with applicable law.

12. DATA BREACH NOTIFICATION

- 12.1 Equipp maintains appropriate logs and monitoring mechanisms to detect personal data breaches. In the event of a personal data breach, Equipp will assess the nature and scope of the breach and take prompt remedial measures.

- 12.2 Where a personal data breach is required to be notified under the DPDP Act and DPDP Rules, Equipp will notify the Data Protection Board of India and, where required, affected data principals, in accordance with the timelines and procedures prescribed under applicable law. Notifications will include the information required under the DPDP Rules, including the nature of the breach, the categories of data affected, and the remedial steps taken or proposed.

13. UPDATES TO THIS PRIVACY POLICY

- 13.1 Equipp may amend this Privacy Policy from time to time to reflect changes in applicable law, regulatory guidance, technology, or its operational practices. Updated versions will be published on the Platform with a revised Effective Date.

- 13.2 Where required by applicable law or the nature of the change, Equipp will provide appropriate advance notice of material amendments or seek renewed consent. Continued use of the Services after the Effective Date of an updated Privacy Policy constitutes deemed acceptance of the updated terms, consistent with the clickwrap and master relationship approach used in the Customer Agreements. Customers are encouraged to review this Privacy Policy periodically.

By clicking "I Agree", checking the applicable consent box, or continuing to use the Services, you confirm that you have read, understood, and consent to this Privacy Policy.