

IOTAMINE CLOUD PRIVATE LIMITED

C/o WeWork DLF Forum, Cybercity, Phase-III, DLF QE, Gurgaon, Haryana - 122002
CIN: U62099HR2025PTC131427 · Email: corporate@iotamine.com

PRIVACY POLICY

Notice under Section 5 of the Digital Personal Data Protection Act, 2023, read with Rule 3 of the Digital Personal Data Protection Rules, 2025

Version: 2.0

Effective date: 14 October 2026

Governing law: India

1. INTRODUCTION AND SCOPE

- 1.1 This Privacy Policy ("Policy") is issued by Iotamine Cloud Private Limited, a company incorporated under the Companies Act, 2013, bearing Corporate Identity Number U62099HR2025PTC131427 and having its registered office at C/O WeWork DLF Forum, Cybercity, Phase III, DLF QE, Gurgaon, Haryana, India, 122002 ("Iotamine", "we", "us" or "our"), and applies to the processing of personal data in connection with iotamine.com, the Iotamine control panel, our application programming interfaces and integrations, and the cloud services we provide (collectively, the "Services").
- 1.2 In respect of the personal data described in this Policy, Iotamine is the **Data Fiduciary** within the meaning of Section 2(i) of the DPDP Act.
- 1.3 This Policy does not govern Customer Content. Where Customer Content contains personal data of any individual, you are the Data Fiduciary in respect of such personal data and Iotamine acts as your Data Processor, processing it solely to provide the Services, on your documented instructions, or as required by law.
- 1.4 This Policy should be read together with our Terms of Service and Acceptable Use Policy.

2. DEFINITIONS

- 2.1 In this Policy, unless the context otherwise requires, the following terms have the meanings given below. Terms not defined here have the meanings given to them in the DPDP Act.

“**DPDP Act**” means the Digital Personal Data Protection Act, 2023, as amended from time to time.

“**DPDP Rules**” means the Digital Personal Data Protection Rules, 2025, as amended from time to time.

“**Personal data**” means any data about an individual who is identifiable by or in relation to such data.

“**Data Principal**” means the individual to whom the personal data relates, referred to in this Policy as "you".

“**Data Fiduciary**” means a person who alone or with others determines the purpose and means of processing personal data.

“**Data Processor**” means a person who processes personal data on behalf of a Data Fiduciary.

“**Customer Content**” means all data, including files, databases and software, that you store or process using the Services.

“**Board**” means the Data Protection Board of India established under the DPDP Act.

3. PERSONAL DATA COLLECTED AND PURPOSES OF PROCESSING

- 3.1 We process the categories of personal data set out below, for the purposes and on the lawful basis indicated against each. "Consent" refers to consent given under Section 6 of the DPDP Act. "Legitimate use" refers to a use permitted under Section 7 of the DPDP Act, including personal data provided voluntarily for a specified purpose. "Required by law" refers to processing necessary to comply with a legal obligation.

No.	Category	Personal data	Purpose	Basis
3.1.1	Account and contact details	Name, email address, phone number, login credentials, and business and billing details you provide (such as company name, address and tax registration).	Creating and managing your account, authentication, invoicing, and communicating with you regarding your account and the Services.	CONSENT
3.1.2	Payment and billing information	Transaction details such as amount, date, payment reference and invoices. Card, UPI and bank details are processed by our payment partners and are not stored by us.	Processing payments, maintaining your account balance, invoicing, and compliance with accounting and tax obligations.	LEGITIMATE USE; REQUIRED BY LAW
3.1.3	Identity verification (KYC)	Identity details obtained with your consent through government-recognised methods such as DigiLocker or Aadhaar, like name, date of birth, gender and address. Your full Aadhaar number is not stored.	Verifying your identity as required of cloud service providers under applicable law, preventing fraud and misuse, and determining eligibility for promotional offers.	CONSENT; REQUIRED BY LAW
3.1.4	Technical and security information	IP address, device and browser information, sign-in records, and a record of actions taken on your account.	Securing your account and our network, detecting and investigating fraud and abuse, and maintaining records required by law.	LEGITIMATE USE; REQUIRED BY LAW

No.	Category	Personal data	Purpose	Basis
3.1.5	Service and usage information	Resources you use, their configuration and usage (compute, storage, bandwidth), and commands or file operations run on your servers through our tools.	Providing and operating the Services, accurate billing, making your usage and history available to you, and capacity planning.	LEGITIMATE USE
3.1.6	Support communications	Messages, requests and attachments you send to our support team, and our replies.	Responding to your requests and resolving issues. Automated tools may assist in preparing replies; all replies are reviewed by our staff before they are sent.	LEGITIMATE USE
3.1.7	Website usage and advertising measurement	How you use our website and control panel (pages visited, features used), how you found us (referring site, or the identifier of the advertisement you clicked), and approximate location at city level. This is collected only by our own analytics: we do not use third-party tracking scripts, and we do not store your IP address or full browser details for this purpose.	Improving our website and Services, and measuring our marketing. Before you create an account, this information is held against a random identifier and is not used to identify you; when you create an account, it is linked to your account. When an advertisement results in a sign-up or purchase, we inform the advertising platform concerned from our servers, using the advertisement click identifier and, where the platform requires it, your email address or phone number in hashed form.	CONSENT

3.2 We shall not process personal data for any purpose other than those specified in this Policy without first notifying you and, where required by law, obtaining your consent.

3.3 Card, UPI and bank account details are collected and processed directly by our payment partners and are not stored by Iotamine. Your full Aadhaar number is not stored by Iotamine.

4. **CONSENT AND WITHDRAWAL OF CONSENT**

4.1 Where processing is based on consent, such consent is obtained through a clear affirmative action, including your acceptance of this Policy and the Terms of Service at the time of registration, or when you complete a specific action such as identity verification.

- 4.2 You may withdraw your consent at any time, with the same ease with which it was given, by writing to the Grievance Officer or, in the case of website analytics, by using the control provided in clause 13.3.
- 4.3 Withdrawal of consent shall not affect the lawfulness of processing carried out before such withdrawal. Where the Services depend on the personal data concerned, withdrawal may result in our being unable to continue providing those Services, in which case your account may be closed in accordance with the Terms of Service.
- 4.4 You may also give, manage, review or withdraw consent through a Consent Manager registered with the Data Protection Board of India, once such facility is available.

5. DISCLOSURE OF PERSONAL DATA

- 5.1 We disclose personal data only to the extent necessary, to the categories of recipients below. Each Data Processor engaged by us acts under a valid contract and processes personal data only for the purpose for which it is engaged.

Category of recipient	Purpose
Payment processors	Processing payments and refunds
Identity verification providers	Completing KYC verification
Communication service providers	Sending emails and service notifications
Infrastructure and security providers	Hosting, delivering and protecting our websites and Services
Advertising platforms	Measuring whether our advertisements result in sign-ups or purchases, using click identifiers and hashed contact details sent from our servers
Software and AI service providers	Supporting our operations, including assistance in preparing support replies
Professional advisers	Legal, accounting and audit services
Authorities	Where required by law, including CERT-In, courts, regulators and law-enforcement agencies acting under a valid order

- 5.2 **Business transfers.** In the event of a merger, demerger, acquisition or transfer of all or part of our business, personal data may be transferred to the successor entity. We shall notify you before your personal data becomes subject to a different privacy policy.
- 5.3 **At your direction.** Where you connect a third-party application or integration to your account, such application acts with the access you authorise.
- 5.4 Iotamine does not sell personal data. Upon request under clause 8, we shall provide the identities of the Data Fiduciaries and Data Processors with whom your personal data has been shared.

6. TRANSFER OF PERSONAL DATA OUTSIDE INDIA

Stored in india. Account data is stored on systems located in India.

Processed abroad. Certain service providers process personal data in the United States and other countries.

- 6.1 Transfers of personal data outside India are made in accordance with Section 16 of the DPDP Act. We shall not transfer personal data to any country or territory notified as restricted by the Central Government.
- 6.2 Where you elect to deploy resources in a region outside India, Customer Content stored in such resources is held in that region.

7. RETENTION OF PERSONAL DATA

- 7.1 In accordance with Section 8(7) of the DPDP Act, we retain personal data only for as long as necessary for the purposes for which it was collected, or for such longer period as is required by applicable law, as set out below. Upon expiry of the applicable period, personal data is erased or irreversibly anonymised.

Personal data	Retention period	Basis for retention
Command output	Up to 30 days	Reviewing changes to your servers
Ad click identifiers	Up to 90 days	Measuring marketing
Security and access logs	1 year	DPDP Rules, 2025 and CERT-In Directions, 2022
Website usage data	Up to 13 months	Improving the website
Support communications	Account life + 3 years	Follow-ups and disputes
KYC records	5 years after closure	CERT-In Directions, 2022
Invoices and tax records	8 years	Companies Act, 2013 and GST law
Account details	While your account is open	Providing the Services
Customer Content and backups	Until deleted by you	Provision of the Services

8. RIGHTS OF DATA PRINCIPALS

- 8.1 Subject to the DPDP Act and the DPDP Rules, you have the following rights in respect of your personal data:
- (a) **Right to access information** (Section 11): To obtain a summary of the personal data being processed, the processing activities undertaken, and the identities of those with whom it has been shared.
- (b) **Right to correction** (Section 12): To have inaccurate or misleading personal data corrected, and incomplete personal data completed or updated.

- (c) **Right to erasure** (Section 12): To have personal data erased once it is no longer necessary for the purpose for which it was processed, unless retention is required by law.
- (d) **Right to withdraw consent** (Section 6(4)): To withdraw consent at any time, with the same ease with which it was given.
- (e) **Right of grievance redressal** (Section 13): To have grievances addressed by our Grievance Officer in accordance with clause 10.
- (f) **Right to nominate** (Section 14): To nominate another individual to exercise your rights in the event of your death or incapacity.

8.2 **Procedure.** Requests to exercise these rights shall be made to the Grievance Officer at corporate@iotamine.com from the email address registered to your account.

- (i) **Submit request.** Write to the Grievance Officer from your registered email, stating the right you wish to exercise.
- (ii) **Verification.** We may verify your identity to protect your personal data from unauthorised requests.
- (iii) **Action.** We act on your request in accordance with the DPDP Act and the DPDP Rules.
- (iv) **Response.** You receive our response within ninety (90) days of receipt of your request.

8.3 **Time period.** We shall respond to your request within **ninety (90) days** of its receipt, in accordance with the DPDP Rules. We may verify your identity before acting on a request.

8.4 **Limitations.** The right to erasure does not extend to personal data that we are required to retain under applicable law, including the records specified in clause 7.

9. DUTIES OF DATA PRINCIPALS

9.1 In accordance with Section 15 of the DPDP Act, while exercising your rights you shall:

- (a) comply with all applicable laws;
- (b) not impersonate another person while providing your personal data;
- (c) not suppress any material information while providing personal data for identity verification;
- (d) not register a false or frivolous grievance or complaint; and
- (e) furnish only verifiably authentic information when seeking correction or erasure.

10. GRIEVANCE REDRESSAL

- (i) **Grievance Officer.** Grievances may be addressed to corporate@iotamine.com. We shall acknowledge and resolve your grievance within **ninety (90) days**.
- (ii) **Data Protection Board of India.** If your grievance is not resolved, you may file a complaint with the Board. Information is available on the Ministry of Electronics and IT website (<https://www.meity.gov.in/data-protection-framework>).

- 10.1 In accordance with Section 13(3) of the DPDP Act, you are required to exhaust the grievance redressal mechanism provided by Iotamine before approaching the Data Protection Board of India.

11. PROCESSING OF CHILDREN'S PERSONAL DATA

- 11.1 The Services are intended only for persons who have attained the age of **eighteen (18) years**. In accordance with Section 9 of the DPDP Act, we do not knowingly process the personal data of a child, and we do not undertake tracking, behavioural monitoring or targeted advertising directed at children.
- 11.2 If we become aware that an account belongs to a child, we shall close the account and erase the associated personal data, save as required to be retained by law.

12. SECURITY SAFEGUARDS AND PERSONAL DATA BREACH

- 12.1 In accordance with Section 8(5) of the DPDP Act and Rule 6 of the DPDP Rules, we maintain reasonable security safeguards to prevent personal data breach, including:

Safeguard	Description
Encryption in transit	Personal data transmitted between you and the Services is encrypted in transit.
Protection of identifiers	Credentials and sensitive identifiers are stored in hashed or masked form.
Access control	Access to personal data is limited to authorised personnel on a need-to-know basis and is logged.
Logging and monitoring	Logging and monitoring are maintained to detect and investigate misuse.

- 12.2 In the event of a personal data breach, we shall notify affected Data Principals and the relevant authorities as set out below, in accordance with Section 8(6) of the DPDP Act and Rule 7 of the DPDP Rules:

Breach notification.

Timing	Notified to	Content
Without delay	Affected Data Principals	The nature, extent and timing of the breach, its likely consequences, mitigation measures, and steps you may take.
Within 72 hours	Data Protection Board of India	Intimation without delay, followed by a detailed report within seventy-two (72) hours.
As prescribed	CERT-In	Reporting within the period prescribed under its directions.

- 12.3 You are responsible for maintaining the confidentiality of your account credentials and API keys. We recommend that you enable two-factor authentication.

13. COOKIES AND SIMILAR TECHNOLOGIES

- 13.1 We use first-party cookies and similar technologies, including browser storage, on our website and control panel, as described below. We do not use third-party cookies or third-party tracking scripts.

Type	Purpose	Duration
Strictly necessary	Required to keep you signed in, secure the Services, and remember settings such as display preferences.	Session
Analytics	A random identifier used by our own analytics to understand how the website is used. It is not shared with any third party.	Up to 13 months
Advertising measurement	Stores the click identifier of the advertisement that brought you to our website, so that we can tell the advertising platform when it results in a sign-up or purchase. It is not read by any third party.	Up to 90 days

- 13.2 Strictly necessary cookies are required for the operation of the Services and cannot be disabled through this page. Disabling them in your browser will prevent you from signing in to the control panel.
- 13.3 You may switch off website analytics for a browser using the control provided in the online version of this Policy at iotamine.com/legal/privacy-policy, and you may manage or delete cookies through your browser settings at any time.

14. AMENDMENTS TO THIS POLICY

- 14.1 We may amend this Policy from time to time. The effective date and version number shown on this page will be updated upon each amendment.
- 14.2 Where an amendment materially affects the manner in which we process your personal data, we shall notify you by email before it takes effect and, where required by law, seek your consent afresh.
- 14.3 Each version of this Policy remains available below in PDF form, so that you can refer to the terms in force on any given date.

Version	Status	Period
v2.0	Current version	Effective from 14 October 2026
v1.0	Superseded	In force 30 April 2025 to 13 October 2026

15. GOVERNING LAW AND INTERPRETATION

- 15.1 This Policy shall be governed by and construed in accordance with the laws of India. Subject to the jurisdiction of the Data Protection Board of India under the DPDP Act, all disputes arising out of or in connection with this Policy shall be subject to the exclusive jurisdiction of the competent courts in India.
- 15.2 This Policy is available in English and, on request, in any language specified in the Eighth Schedule to the Constitution of India. In the event of any inconsistency between versions, the English version shall prevail to the extent permitted by law.
- 15.3 Headings and summaries are for convenience only and shall not affect the interpretation of this Policy.

16. CONTACT DETAILS OF THE GRIEVANCE OFFICER

- 16.1 In accordance with Section 8(9) of the DPDP Act and Rule 9 of the DPDP Rules, questions about the processing of your personal data, requests to exercise your rights, and grievances may be addressed to:

Piyush Ladhar

Director, Founder & CEO · DIN 10247380

Iotamine Cloud Private Limited

Registered office: C/O WeWork DLF Forum, Cybercity, Phase III, DLF QE, Gurgaon, Haryana, India, 122002

CIN U62099HR2025PTC131427

Email: corporate@iotamine.com

Issued by Iotamine Cloud Private Limited (CIN U62099HR2025PTC131427). The current version of this Policy is published at iotamine.com/legal/privacy-policy, which prevails over any copy.

*** END OF DOCUMENT ***