

PRIVACY POLICY

IngeneroX Platform Website and Business Operations Ingenero Technologies (India) Private Limited

1. Introduction

Ingenero Technologies (India) Private Limited ("**Ingenero**", "**we**", "**us**" or "**our**") respects your privacy and is committed to protecting personal data entrusted to us. This Privacy Policy explains what personal data we collect, why we collect it, how we use, share, transfer, retain and protect it, and what rights and choices you have in relation to it.

This Privacy Policy applies to:

- the Ingenero and IngeneroX websites, sub-domains, portals, documentation libraries, knowledge bases and other online properties that link to this Privacy Policy (each, a "**Site**");
- our marketing, events, webinars, demonstrations, bid and tender participation, and other business development activities;
- our dealings with customers, prospective customers, partners, system integrators, resellers, suppliers and their personnel; and
- applications for employment with Ingenero, to the extent submitted through the Site.

This Privacy Policy does not govern the operational data processed inside the IngeneroX Platform on behalf of our customers. That data — including process data, sensor and historian data, and any personal data contained within a customer's environment — is processed under the direction of the customer and is governed by the applicable Platform Access and Product License Agreement, Order Form and any associated data processing terms. Section 4 explains this distinction in detail.

Please read this Privacy Policy together with our **Terms of Use** and our **Cookie Notice**

2. Who We Are and How to Contact Us

	Details
Legal entity	Ingenero Technologies (India) Private Limited
CIN	U51900MH2000FTC128454
Registered office	Unit No. 2, 8th Floor, A Wing, i Think Techno Campus, Pokhran Road No. 2, Thane (West), Maharashtra 400 607, India
How to reach us	Through the contact route published on our website, or in writing to the registered office address above, marked for the attention of the Legal Department.

For the purposes of the **Digital Personal Data Protection Act, 2023** (India), Ingenero acts as a **Data Fiduciary** in respect of the personal data described in Section 5 of this Privacy Policy, and you are the **Data Principal**. For the purposes of the **EU General Data Protection Regulation** and the **UK GDPR**, where applicable to our processing, Ingenero acts as a **controller** in respect of that data.

Where Ingenero processes personal data contained within a customer's IngeneroX environment, Ingenero acts as a **processor** (GDPR/UK GDPR) or as a **Data Processor** (DPDP Act) on behalf of that customer, who is the controller or Data Fiduciary. See Section 4.

Individuals in the European Economic Area or the United Kingdom may contact us in relation to any matter arising under this Privacy Policy using the details in Section 18.

3. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, our services, or applicable law. The "Last Revised" date above shows when it was most recently changed. Where a change is material, we will provide additional notice — for example, by a prominent notice on the Site or by email to registered users — and, where required by law, we will obtain your consent. We encourage you to review this Privacy Policy periodically.

A record of previous versions is available on request.

4. Two Distinct Categories of Data

Because IngeneroX is an industrial platform deployed inside customer environments, it is important to distinguish clearly between two categories of data. Confusing them is the most common source of misunderstanding in industrial software privacy notices.

	Category A — Business and Website Data	Category B — Customer Platform Data
What it is	Personal data about website visitors, enquirers, event attendees, customer and partner personnel, suppliers and job applicants — such as name, business email, job title, employer, and website usage data.	Operational, process, real-time, sensor, historian, alarm, laboratory and configuration data ingested into or generated by the IngeneroX Platform, together with any personal data incidentally contained within it (for example, operator user IDs, shift log entries, alarm acknowledgements or round-sheet entries).
Ingenero's role	Data Fiduciary (DPDP Act) / controller (GDPR). We determine why and how it is processed.	Data Processor (DPDP Act) / processor (GDPR). We process it only on the documented instructions of the customer.
Governed by	This Privacy Policy.	The Platform Access and Product License Agreement, the applicable Order Form and any associated data processing terms. Under that agreement the customer retains exclusive ownership of its process data, and Ingenero is authorised to process it only to operate, support and maintain the Platform for that customer.
Your rights	Exercise directly with Ingenero — see Section 14.	Exercise with the customer organisation that operates the environment. If you contact us directly, we will refer you to that customer and assist them in responding.

The remainder of this Privacy Policy addresses **Category A** unless expressly stated otherwise. Section 10 addresses Category B.

5. Personal Data We Collect

We collect the following categories of personal data:

Category	Examples
Identity and contact data	Full name, job title, function, employer or organisation, business email address, business telephone or mobile number, business postal address, country and region, professional profile links.
Commercial and relationship data	Enquiry and demonstration requests, areas of interest, plant or asset types, correspondence and meeting notes, bid and tender participation records, contract and purchase order administrative details, licence and entitlement records, named-user allocations, support tickets and their contents.
Account and access data	Username, credential and authentication metadata (we do not store passwords in plain text), single sign-on identifiers, multi-factor authentication status, role and permission assignments, licence keys allocated to you, session and login records.
Technical and usage data	IP address, approximate location derived from IP address, device and browser type and version, operating system, screen resolution, language and time zone settings, referring and exit URLs, pages and documents viewed, features used, search terms entered, time and duration of visits, and clickstream data.
Marketing and communications data	Subscription and consent status and history, communication preferences, email open and click events, webinar and event registration and attendance, content downloads, survey and feedback responses.
Event and visitor data	Registration details for events, conferences, webinars and site visits; dietary or accessibility requirements you choose to provide; visitor logs and, where applicable and notified, CCTV footage at our premises.
Recruitment data	Curriculum vitae, employment and education history, references, right-to-work information and other data you submit when applying for a role.
Compliance and screening data	Information required for sanctions, denied-party, export control, anti-bribery and know-your-customer screening of counterparties and their representatives.

Sensitive and special category data. We do not seek to collect special category personal data (as defined under the GDPR) or sensitive personal data in the ordinary course of our business, and we ask that you do not provide it to us. Where we do process such data — for example, accessibility or dietary requirements for an event, or health information supporting a workplace adjustment — we do so only with your explicit consent or where otherwise permitted by law, and we limit access and retention accordingly.

Children. Our Site and our services are directed exclusively at business users and are not intended for children. We do not knowingly collect personal data from any individual under eighteen (18) years of age. If we become aware that we have collected such data without the verifiable consent of a parent or lawful guardian, we will delete it promptly. In accordance with the Digital Personal Data Protection Act, 2023, we do not undertake tracking, behavioural monitoring or targeted advertising directed at children. If you believe a child has provided us with personal data, please contact us using the details in Section 18.

6. How We Collect Personal Data

We collect personal data in the following ways:

- **Directly from you** — when you complete a form on the Site, request a demonstration or quotation, subscribe to communications, register for an event or webinar, download gated content, create an account, raise a support ticket, correspond with us, meet with our personnel, or apply for a role.
- **Automatically** — through cookies, tags, pixels, server logs, software development kits and similar technologies, as described in Section 8 and in our Cookie Notice.

- **From your organisation** — where your employer, client or principal provides your business contact details in connection with a contract, tender, project, licence allocation, support entitlement or partnership.
- **From third parties and public sources** — including business contact data providers, professional networking platforms, marketing and event partners, channel partners and resellers, cloud marketplace operators, public registries, tender and procurement portals, and sanctions and compliance screening databases.

Where we obtain your personal data from a source other than you, we will provide you with notice of that fact and of the source within a reasonable period, and in any event within one month, unless an exemption under applicable law applies.

7. Why We Use Personal Data and Our Legal Basis

We use personal data only for the purposes described below. The table sets out our legal basis under the GDPR and UK GDPR, where applicable, alongside the corresponding position under the Digital Personal Data Protection Act, 2023, under which processing is generally permitted on the basis of consent or of certain specified legitimate uses.

Purpose	What this involves	Legal basis (GDPR / UK GDPR) and DPDP position
Responding to enquiries	Answering questions, arranging demonstrations, preparing quotations and proposals, and following up.	Steps at your request prior to entering a contract; legitimate interests in responding to business enquiries. DPDP: consent, or the specified legitimate use of voluntary provision of data for a stated purpose.
Providing and administering the Site and Registered Areas	Creating and managing accounts, authenticating users, delivering documentation and downloads, and providing support.	Performance of a contract; legitimate interests in operating our services. DPDP: consent / performance of a contract with the Data Principal or their employer.
Contract and account management	Administering licences, entitlements, named users, renewals, invoicing, delivery and support obligations.	Performance of a contract; legitimate interests in managing customer, partner and supplier relationships. DPDP: consent / contractual necessity.
Service communications	Sending release notes, security advisories, end-of-support notices, maintenance windows, incident notifications and policy changes.	Performance of a contract; legal obligation; legitimate interests in keeping users informed of matters affecting operational and security posture. DPDP: specified legitimate use.
Marketing communications	Sending newsletters, event invitations, product announcements and industry content, and inviting you to webinars.	Consent, where required; otherwise legitimate interests in business-to-business marketing to relevant professional contacts, subject always to your right to object or unsubscribe. DPDP: consent.
Analytics and improvement	Understanding how the Site and our content are used, measuring campaign performance, and improving structure, content and usability.	Consent for non-essential cookies and similar technologies; legitimate interests in improving our services. DPDP: consent.

Purpose	What this involves	Legal basis (GDPR / UK GDPR) and DPDP position
Security, integrity and abuse prevention	Monitoring for unauthorised access, scraping, credential abuse, fraud and malicious activity; maintaining logs; conducting investigations.	Legal obligation; legitimate interests in protecting our systems, our intellectual property and our users. DPDP: specified legitimate use.
Compliance and legal	Sanctions, export control, denied-party, anti-bribery and know-your-customer screening; responding to regulators and lawful requests; establishing, exercising or defending legal claims; audit and record-keeping.	Legal obligation; legitimate interests in compliance and in protecting our legal position. DPDP: compliance with law; legal proceedings.
Recruitment	Assessing applications, conducting interviews, verifying credentials and communicating with candidates.	Steps at your request prior to entering a contract; legitimate interests in recruitment; consent for talent pool retention. DPDP: consent / employment purposes.
Corporate transactions	Evaluating, negotiating and completing a merger, acquisition, investment, financing or reorganisation.	Legitimate interests in conducting corporate transactions. DPDP: specified legitimate use, subject to applicable safeguards.

Legitimate interests balancing. Where we rely on legitimate interests, we have assessed whether those interests are overridden by your interests, rights and freedoms. You may request a summary of the relevant balancing assessment by contacting us using the details in Section 18.

Change of purpose. We will use personal data only for the purposes for which it was collected, unless we reasonably consider that a new purpose is compatible with the original purpose, or unless we are otherwise required or permitted by law. Where a new purpose is not compatible, we will provide a fresh notice and, where required, obtain your consent.

8. Cookies, Analytics and Similar Technologies

The Site uses cookies and similar technologies — including pixels, tags, web beacons, local storage and software development kits — to operate the Site, remember your preferences, measure usage and, where you consent, support marketing.

We use the following categories:

- **Strictly necessary** — required for the Site to function, including session management, authentication, load balancing, security and consent-preference storage. These cannot be disabled through our preference tool.
- **Functional** — remember your choices such as language, region and display preferences.
- **Analytics and performance** — help us understand how the Site is used so that we can improve it, including page views, navigation paths, content engagement and error diagnostics.
- **Marketing and advertising** — used to measure campaign effectiveness and, where permitted, to deliver relevant content and advertising on third-party platforms. These may involve the setting of cookies by third parties.

Where required by applicable law, non-essential cookies are set only after you have given consent through our cookie banner or preference centre. You may withdraw or change your consent at any time using the preference

centre and you may also block or delete cookies through your browser settings. Disabling cookies may affect the availability or functionality of parts of the Site.

Do Not Track. Browsers may transmit "Do Not Track" signals. There is no accepted industry standard for responding to them, and we do not currently respond to them.

A current list of the specific cookies and similar technologies in use, their providers, purposes and retention periods, is set out in our Cookie Notice.

9. Marketing Communications and Your Choices

We may send you information about our products, services, events and industry content where you have consented or where we are otherwise permitted to do so under applicable law in a business-to-business context.

You may opt out at any time by using the unsubscribe or preference-management link in any marketing email, by adjusting your preferences in your account or preference centre, or by contacting us using the details in Section 18. Opting out of marketing does not stop service, transactional, security, contractual or legally required communications, which we may continue to send while your relationship with us subsists.

We do not sell personal data, and we do not rent or lease our contact lists to third parties.

10. Customer Platform Data (Ingenero as Processor)

Where a customer deploys the IngeneroX Platform — on-premise, in the customer's own cloud tenancy, or in a cloud environment managed by Ingenero or a technology partner — the data within that environment is the customer's data. This includes process, sensor, historian, alarm, laboratory, maintenance and configuration data, and any personal data incidentally contained within it, such as operator or engineer user identifiers, shift log entries, alarm acknowledgements, round-sheet entries and audit trail records.

In respect of that data:

- the **customer** is the Data Fiduciary or controller and determines the purposes and means of processing;
- **Ingenero acts only as a Data Processor or processor**, and processes such data solely on the customer's documented instructions and solely to deliver, support, secure, host and maintain the Platform for that customer;
- Ingenero does not sell, rent, lease or use such data for its own marketing purposes;
- Ingenero personnel and authorised subcontractors access such data only where necessary — for example, for implementation, configuration, incident diagnosis, support or maintenance — under confidentiality obligations, role-based access controls and, where deployed, session logging and just-in-time access approval;
- the customer is responsible for the lawfulness of the data it makes available to the Platform, for providing any required notices to its own personnel, for obtaining any required consents, and for responding to requests from individuals whose data is held in its environment; and
- the customer is responsible for data residency, sovereign storage, archival and retention obligations applicable to its own regulatory environment.

Ingenero will assist customers, so far as reasonably practicable, in responding to requests from individuals and to regulators, and in meeting their security, breach notification and data protection impact assessment obligations, in each case as set out in the applicable agreement.

If you are an employee, contractor or representative of an Ingenero customer and wish to exercise rights in relation to data held in your organisation's IngeneroX environment, please contact your organisation directly. If you contact us, we will refer your request to the relevant customer and assist them in responding.

11. Artificial Intelligence, Machine Learning and Model Training

Ingenero develops and operates artificial intelligence and machine learning capabilities, including analytics models, anomaly detection, soft sensors, optimisation routines and retrieval-augmented generation components such as PEnAI. In relation to personal data and AI:

- **We do not use customer process data or customer platform data to train, fine-tune or improve models made available to other customers**, except where a customer has expressly agreed in writing, and then only using anonymised or aggregated data from which individuals and the customer cannot reasonably be identified.
- We may use aggregated and anonymised usage statistics, telemetry and diagnostic information to improve model quality, platform performance and reliability. Such information does not identify you or your organisation.
- Where AI features on the Site process your inputs, those inputs may be logged and reviewed for security, abuse prevention and quality assurance. Please do not submit personal data, confidential information or credentials into such features.
- Where third-party model providers are used, we contract to prohibit them from using inputs or outputs to train their own models, and we bind them by confidentiality and security obligations.

Automated decision-making. We do not make decisions producing legal effects concerning you, or similarly significantly affecting you, based solely on automated processing of your personal data. Analytics outputs generated by the IngeneroX Platform are directed at industrial process and equipment behaviour, not at individuals. Where a customer configures the Platform in a manner that involves automated decision-making about individuals, that customer is responsible for the associated notices, safeguards, human review mechanisms and rights.

12. Sharing and Disclosure of Personal Data

We share personal data only as described below, and only with recipients bound by appropriate confidentiality and data protection obligations.

- **Within the Ingenero group** — with our parent, subsidiaries and affiliates, for the purposes described in this Privacy Policy and under intra-group data transfer arrangements.
- **Service providers and sub-processors** — including cloud infrastructure and hosting providers, customer relationship management and marketing automation platforms, email delivery services, analytics providers, ticketing and support platforms, collaboration and productivity suites, event and webinar platforms, payment and accounting service providers, and recruitment systems. These parties process personal data only on our instructions and under written contracts.
- **Professional advisers** — lawyers, auditors, insurers, bankers and consultants, where necessary and subject to professional or contractual confidentiality duties.
- **Channel partners, resellers, distributors and system integrators** — where necessary to respond to an enquiry, deliver a project, or provide support, and where you or your organisation has engaged with us through that party.
- **Customers** — where you are a representative of a customer or partner, we may share your business contact and entitlement details with the contracting organisation for administration purposes.

- **Regulators, courts and authorities** — where we are required to do so by applicable law, regulation, legal process or an enforceable governmental request, or where necessary to establish, exercise or defend legal claims, to enforce our agreements, or to protect the rights, property or safety of Ingenero, our users or the public.
- **Acquirers and investors** — in connection with any actual or proposed merger, acquisition, investment, financing, reorganisation or sale of assets, subject to appropriate confidentiality protections. Where personal data is transferred as part of such a transaction, the recipient will be bound to use it consistently with this Privacy Policy.

We do not sell personal data, and we do not share personal data for cross-context behavioural advertising as those terms are defined under California law, except to the extent that the use of certain third-party marketing cookies with your consent may be treated as "sharing" under that law. You may exercise the choices described in Sections 8 and 14.5.

A current list of the sub-processors we engage is available on request and, for customers, is maintained under the applicable Platform Agreement.

13. International Transfers

Ingenero operates internationally and engages service providers in multiple countries. Personal data collected through the Site or in the course of our business may therefore be transferred to, stored in, or accessed from countries other than the one in which it was collected, which may include **India, the United States, the European Economic Area, the United Kingdom, Singapore and the United Arab Emirates**, depending on the systems and providers involved.

Some of these countries may not provide the same level of data protection as your own. Where we transfer personal data internationally, we implement appropriate safeguards, which may include:

- the **European Commission's Standard Contractual Clauses** and, for UK transfers, the UK International Data Transfer Agreement or Addendum, supported by transfer impact assessments where required;
- an **adequacy decision** by a competent authority in respect of the recipient country;
- intra-group data transfer agreements incorporating equivalent protections; and
- contractual, technical and organisational measures including encryption in transit and at rest, access controls, pseudonymisation where practicable, and restrictions on onward transfer.

Under the **Digital Personal Data Protection Act, 2023**, transfers of personal data outside India are permitted except to territories notified as restricted by the Central Government. We monitor such notifications and will adjust our transfer arrangements accordingly.

You may request further information about the safeguards applied to a particular transfer by contacting us using the details in Section 18.

14. Your Rights and Choices

Your rights depend on the law applicable to you. Where more than one regime applies, we will apply the more protective standard. We do not discriminate against you for exercising any right.

14.1 Rights under the Digital Personal Data Protection Act, 2023 (India)

- **Right to access information** — to obtain a summary of the personal data being processed, the processing activities undertaken, and the identities of other Data Fiduciaries and Data Processors with whom it has been shared.

- **Right to correction, completion, updating and erasure** — to have inaccurate or misleading data corrected, incomplete data completed, data updated, and data erased where it is no longer necessary for the purpose for which it was collected and no legal obligation requires its retention.
- **Right of grievance redressal** — to a readily available means of raising a grievance with us, which we must respond to within the prescribed period, before approaching the Data Protection Board of India.
- **Right to nominate** — to nominate another individual to exercise your rights in the event of your death or incapacity.
- **Right to withdraw consent** — where processing is based on consent, to withdraw it at any time, with the same ease with which it was given. Withdrawal does not affect the lawfulness of processing before withdrawal, and we may be unable to continue providing certain services following withdrawal.

You also have duties as a Data Principal under the Act, including not to impersonate another person, not to suppress material information, and not to raise false or frivolous grievances.

14.2 Rights under the GDPR and UK GDPR

Where the GDPR or UK GDPR applies to our processing of your personal data, you have the following rights:

- **Access** — to obtain confirmation of whether we process your personal data and a copy of it.
- **Rectification** — to have inaccurate data corrected and incomplete data completed.
- **Erasure** — to have your data deleted where there is no overriding lawful basis for continued processing.
- **Restriction** — to have processing suspended in defined circumstances, including while accuracy or a legitimate interests objection is being verified.
- **Portability** — to receive personal data you provided to us, where processing is based on consent or contract and carried out by automated means, in a structured, commonly used and machine-readable format, and to have it transmitted to another controller where technically feasible.
- **Objection** — to object to processing based on legitimate interests on grounds relating to your particular situation, and an **absolute right to object to processing for direct marketing purposes** at any time.
- **Withdrawal of consent** — at any time, without affecting the lawfulness of prior processing.
- **Complaint** — to lodge a complaint with your local supervisory authority. In the United Kingdom this is the Information Commissioner's Office. We would appreciate the opportunity to address your concerns before you do so.

14.3 Rights under California law

Where the California Consumer Privacy Act, as amended by the California Privacy Rights Act, applies to our processing and you are a California resident, you have the right to know the categories and specific pieces of personal information we have collected, the sources, the business purposes and the categories of recipients; to request deletion; to request correction; to opt out of any sale or sharing of personal information; and to limit the use of sensitive personal information. We do not sell personal information. To exercise these rights, contact us using the details in Section 18. You may use an authorised agent, subject to verification.

14.4 Other jurisdictions

Residents of other jurisdictions may have comparable rights under applicable local law, including under the laws of Singapore, the United Arab Emirates, Saudi Arabia, Brazil, Canada, Australia and other territories in which our customers operate. Please contact us and we will respond in accordance with the law applicable to you.

14.5 How to exercise your rights

To exercise any right, contact us using the details in Section 18, stating clearly the right you wish to exercise and the personal data concerned.

- **Verification.** We will take reasonable steps to verify your identity before acting on a request. We may ask for additional information for this purpose; that information will be used only for verification.
- **Timescales.** We will respond within the period required by applicable law — generally within one month under the GDPR and UK GDPR (extendable by two further months for complex or numerous requests, with notice), and within the prescribed period under the Digital Personal Data Protection Act, 2023.
- **Fees.** We do not charge a fee. We may charge a reasonable fee or refuse to act where a request is manifestly unfounded, excessive or repetitive, and we will explain our reasons.
- **Limits.** Rights are not absolute. We may decline all or part of a request where an exemption applies, including where compliance would prejudice legal claims, breach confidentiality obligations owed to others, or conflict with a legal retention requirement. We will explain any refusal.
- **Platform data.** Requests concerning data held within a customer's IngeneroX environment must be directed to that customer, as explained in Sections 4 and 10.

15. Data Retention

We retain personal data only for as long as necessary for the purposes for which it was collected, including to satisfy legal, accounting, tax, regulatory, audit, contractual, dispute resolution or reporting requirements. In determining the appropriate retention period, we consider the nature, volume and sensitivity of the data, the potential risk of harm from unauthorised use or disclosure, the purposes of processing, whether those purposes can be achieved by other means, and applicable legal requirements.

Our retention periods are as follows:

Data category	Retention period
Enquiry and demonstration request data (no relationship established)	24 months from last interaction, then deleted or anonymised.
Customer, partner and supplier relationship data	Duration of the relationship plus 7 years, to satisfy contractual limitation and statutory record-keeping requirements.
Contract, invoice and financial records	As required by the Companies Act, 2013, Indian tax law and other applicable statutes — generally 8 years.
Account and access records for Registered Areas	Duration of the account plus 12 months after deactivation.
Marketing consent and preference records	For as long as consent subsists, plus 7 years thereafter as evidence of consent and of opt-out compliance.
Website analytics and cookie data	As stated in the Cookie Notice, generally between 13 and 26 months.
Security, access and audit logs	12 to 24 months, or longer where required for an active investigation or legal claim.
Recruitment data (unsuccessful applicants)	12 months from the conclusion of the process, or longer with your consent for talent pool purposes.

Where personal data is no longer required, we securely delete it or irreversibly anonymise it. Anonymised data may be retained and used indefinitely for statistical and analytical purposes. Data held in backups is deleted in accordance with our backup rotation cycle.

16. Security

We implement appropriate technical and organisational measures, and reasonable security safeguards as required under applicable law, to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. These measures include, as applicable to the system concerned:

- encryption of data in transit using industry-standard transport security, and encryption of data at rest;
- role-based access control, least-privilege provisioning, multi-factor authentication and privileged access management;
- network segmentation, firewalling and, in operational technology contexts, architecture aligned to the Purdue reference model and to IEC 62443, including the use of an industrial demilitarised zone;
- logging, monitoring, intrusion detection and endpoint detection and response;
- secure software development practices, code review, dependency and vulnerability management, and periodic security testing;
- vendor and sub-processor security due diligence and contractual security obligations;
- personnel background verification where permitted by law, confidentiality undertakings, and regular security and privacy awareness training; and
- documented incident response, business continuity and disaster recovery procedures, which are tested periodically.

Breach notification. We maintain procedures to detect, investigate and respond to personal data breaches. Where a breach is likely to result in a risk to the rights and freedoms of individuals, we will notify the competent supervisory authority and, where required, affected individuals, in each case within the timescale required by applicable law. Under the Digital Personal Data Protection Act, 2023, we will notify the Data Protection Board of India and each affected Data Principal as prescribed. Where a breach affects a customer's data, we will notify that customer in accordance with the applicable agreement.

No absolute guarantee. No method of transmission over the internet and no method of electronic storage is completely secure. While we strive to protect personal data using commercially reasonable means, we cannot guarantee absolute security, and you acknowledge that there are security and privacy limitations inherent to the internet that are beyond our control. You are responsible for keeping your credentials confidential and for notifying us promptly of any suspected compromise.

17. Third-Party Links and Services

The Site may contain links to third-party websites, platforms, marketplaces and services. We do not control and are not responsible for their content, security or privacy practices. This Privacy Policy does not apply to them. We encourage you to review the privacy notice of any third-party site or service before providing personal data to it.

18. Questions, Concerns and Complaints

If you have any question, concern or complaint about this Privacy Policy or about how we handle personal data, please contact us first — we are committed to working with you to reach a fair resolution.

- Through the contact route published on our website; or

- In writing to: Ingenero Technologies (India) Private Limited, Unit No. 2, 8th Floor, A Wing, i Think Techno Campus, Pokhran Road No. 2, Thane (West), Maharashtra 400 607, India — marked for the attention of the Legal Department.

We will acknowledge a complaint within twenty-four (24) hours of receipt and will endeavour to resolve it within fifteen (15) days of receipt, or within such shorter period as applicable law may require.

If you are not satisfied with our response, you have the right to complain to the competent authority: the **Data Protection Board of India** (for individuals in India), your local **supervisory authority** in the European Economic Area, the **Information Commissioner's Office** in the United Kingdom, or the relevant authority in your jurisdiction.

© 2026 Ingenero Technologies (India) Private Limited. All rights reserved. IngeneroX and the IngeneroX module names are trademarks of Ingenero Technologies (India) Private Limited.