

Privacy Policy

Effective Date: 01-05-2025

Sanchai Analytics Pvt Ltd, referred to as “Sanchai Analytics” in this document, is an India-based AI company deploying agentic AI products in Industrial plants. This framework outlines a comprehensive approach to privacy and cybersecurity, ensuring compliance with Indian laws and global best practices. It includes a customer-facing Privacy Policy, internal data governance measures, cloud security controls, guidelines for integrating Large Language Model (LLM) APIs, and recommendations for industry certifications. Implementation checklists and planning tables are provided to guide practical adoption.

1. Customer-Facing Privacy Policy (DPDP Act Compliance and Global Principles) [🔗](#)

Introduction: Sanchai Analytics Pvt. Ltd. is committed to protecting personal data and sensitive industrial information. This Privacy Policy explains what data we collect, how we use and safeguard it, and the rights of individuals. It is designed to comply with India's Digital Personal Data Protection Act (DPDP Act) 2023 and globally recognized principles of privacy and data protection.

Scope: This policy applies to all personal data collected through Sanchai Analytics' AI products and services. "Personal Data" means any data about an identifiable individual in digital form. It covers personal identifiers (like names, emails) and any plant or operational data linked to individuals. Industrial data (sensor measurements, operational logs, files) that is not identifiable to an individual is treated as confidential business information, though not "personal data" under DPDP.

Information We Collect [🔗](#)

- **Personal Identifiers:** Name, username, email address, contact information, and organizational details provided during account creation or use of our services.
- **Usage Data:** Logs of user interactions with the AI system, such as query inputs, AI outputs, timestamps, and user feedback. This may include plant names or device IDs if included in prompts.
- **Device and Technical Data:** Information like IP address, browser type, and operating environment, collected via the user interface for security and debugging purposes.
- **Industrial Data Inputs:** Data from manufacturing operations that stream into the AI platform (e.g. sensor readings, production logs, configuration files). While not personal data, we protect such data as sensitive and contractually confidential to our clients.

Purpose of Processing and Use of Data [🔗](#)

We process personal and industrial data solely for legitimate business purposes and with consent or other lawful basis. The primary purposes include:

- **Service Delivery:** To analyze plant data and provide AI-driven insights, predictions, or automation in industrial processes as requested by users. For example, personal identifiers are used to authenticate users and attribute their queries, while sensor data is processed to generate analytic outputs.
- **Communication:** To send account notifications, updates, and respond to user inquiries or support requests. Email addresses and names are used for communication on service matters, and only for marketing with explicit consent.
- **Security and Compliance:** To monitor and ensure the security of our services, prevent fraud or abuse, and comply with legal obligations. Operational logs including user actions are reviewed to detect unauthorized access or policy violations (without infringing on user privacy).

We adhere to the principles of *lawfulness, fairness, and transparency* in processing, and *purpose limitation* and *data minimization* – we only collect data necessary for the stated purposes. We also strive for *accuracy* of data, allowing corrections, and *storage limitation* – retaining personal data only as long as needed for those purposes. All processing is backed by *reasonable security safeguards* to prevent unauthorized use or breach. Sanchai Analytics, as the "Data Fiduciary" (controller), is *accountable* for how data is used.

Consent and Choice [🔗](#)

Where consent is the legal basis for processing, we obtain clear and affirmative consent before collecting or using personal data. Users are presented with a consent notice at sign-up or data collection, detailing what personal data is collected and for what purpose, in easy-to-understand language. Consent is voluntary, specific, informed, and unambiguous, and users have the right to withdraw consent at any time. For example, if we ever wish to use personal information for a new purpose, we will seek fresh consent.

By default, Sanchai Analytics will not collect or send **any** personal data to external providers beyond what is necessary to fulfill the user's query.

Children's Data: Our services are intended for business use in industrial settings and not directed at children under 18. We do not knowingly collect personal data from minors. If a client organization includes any users who are minors, the organization must ensure verifiable parental consent in accordance with the DPDP Act's requirements for processing children's data. Sanchai Analytics will not process data likely to cause harm to children or use it for any profiling or targeted advertising towards minors.

Data Sharing and Disclosure [🔗](#)

We do **not** sell or rent personal data to third parties. We only share data under the following circumstances:

- **Service Providers (Processors):** Sanchai Analytics uses reputable cloud hosting and technology providers to operate our platform primarily Microsoft Azure and LLM API providers like OpenAI, Anthropic, Google for AI processing. These third parties process data on our behalf under strict contracts. They are bound to only process data for our instructed purposes and to implement robust security measures. We conduct due diligence to ensure such partners have certifications (e.g. ISO 27001, SOC 2) and comply with privacy laws.
- **LLM API Integration:** When users ask our AI agent complex questions, we relay necessary data to Large Language Model APIs (such as OpenAI, Anthropic Claude, or Google Gemini) to generate natural language responses. **We minimize and anonymize** the data in these requests – for instance, replacing real names or IDs with generic placeholders before sending. The LLM providers are given only the information needed to process the query, and they are **not permitted to use that data for any purpose except to return the result**. Data sent to these AI APIs is always encrypted in transit.
- **Within the Company:** Access to personal data internally at Sanchai Analytics is restricted to personnel who need it to perform their job (e.g. support staff assisting a user query or engineers investigating a technical issue). All staff are bound by confidentiality and trained in data protection.
- **Business Transfers:** In the event of a merger, acquisition, or sale of Sanchai Analytics, personal data may be transferred to the successor entity. In such cases, we will ensure the receiving party is bound to the same level of privacy protection, and users will be notified of any changes to data handling.

Cross-Border Data Transfers: Sanchai Analytics is based in India, but our cloud infrastructure and LLM partners may be located in other countries. Whenever personal data is transferred outside India, we comply with applicable transfer regulations. Under the DPDP Act, personal data transfers are allowed to all countries except any that may be specifically restricted by the Indian government. We will not transfer data to any jurisdiction that is blacklisted once such list is published. For international transfers (for example, to the United States where OpenAI/Anthropic servers may reside), we ensure appropriate safeguards are in place. These include standard contractual clauses or Data Processing Addendum that oblige the recipient to protect the data, and technical measures like encryption. We also prioritize using cloud regions in India or jurisdictions approved by regulators, to the extent possible, for hosting personal data.

Data Retention and Deletion [🔗](#)

We retain personal data only as long as necessary to fulfill the purposes for which it was collected, unless a longer retention is required by law. In practice:

- Account information (names, contact details) is kept for the duration of the customer relationship and deleted upon request or account closure, after fulfilling any legal retention requirements.
- Operational data (logs, sensor inputs) is stored to provide the service. Raw uploaded files or logs can be deleted by the user or upon request. We periodically review and purge data that is no longer needed, to uphold the DPDP principle of storage

limitation.

- Backups containing personal data are secured and retained for limited periods before automated deletion, in accordance with our backup policy. When we delete personal data, we ensure it is removed from all active systems. Some residual data may persist in secure backups for a short time until those are rotated out; such backups remain protected and are not used for any active processing. If deletion is requested or consent withdrawn, we will also instruct our processors to delete the data from their systems where applicable.

Data Security Measures [🔗](#)

We employ **industry-standard security measures** to protect personal and sensitive data from unauthorized access, alteration, or loss. These include:

- **Encryption:** All personal data is encrypted both in transit and at rest. Web interactions use HTTPS/TLS encryption. Sensitive data at rest (databases, file storage) is encrypted using strong algorithms (e.g. AES-256) and managed keys. Encryption keys are stored securely (using cloud key management services and hardware security modules) and rotated regularly.
- **Access Control:** Access to systems storing personal data is limited by role-based access control and multifactor authentication. Only authorized staff and service accounts with least-privilege permissions can access sensitive information, and all access is logged.
- **Monitoring and Auditing:** We maintain detailed logs of access and data processing activities. Our security team uses monitoring tools to detect unusual patterns or unauthorized activities in real time. Regular audits of our systems and processes are conducted to ensure policy compliance and identify improvements.
- **Secure Development:** We follow secure software development life cycle practices, including code reviews, security testing, and vulnerability scanning before deployment. Our DevOps processes incorporate security checks (e.g. dependency scanning, container security) to catch issues early.
- **Incident Response:** Sanchai Analytics has an incident response plan to handle any security or data breach swiftly. If an incident affecting personal data occurs, we will notify affected individuals and authorities as required by law, and take steps to mitigate any harm.
- **Third-Party Security:** We ensure our third-party processors (cloud providers, LLM API services) have robust security postures. This includes reviewing their SOC 2 or ISO 27001 reports and contractual commitments to security. We remain accountable for protecting the data even when processed by these partners.

These measures are continually reviewed and updated in line with evolving threats and best practices. However, no system is 100% secure; we therefore also depend on users to keep their account credentials confidential and report any suspected unauthorized activity.

Individual Rights and Choices [🔗](#)

We honor all rights that individuals (Data Principals) are granted under the DPDP Act and other applicable laws. These include:

- **Right to Access:** You may request a summary of the personal data we hold about you and how we have processed it. This includes information on what data, for what purpose, and which third parties (if any) it has been shared with.
- **Right to Correction:** You have the right to correct or update any of your personal data that is inaccurate or incomplete. We provide self-service editing for basic profile information and will assist with other correction requests.
- **Right to Erasure:** You may request deletion of your personal data that was collected based on consent. If you withdraw consent or terminate services, we will erase your personal data unless we are required to retain it for legal reasons. For example, you can ask us to delete your account and associated data at any time.
- **Right to Withdraw Consent:** Where we rely on your consent, you can withdraw that consent at any point. We make it as easy to withdraw as to give consent (for instance, via an account settings option or by contacting us). Withdrawal will not affect the lawfulness of processing already done, but we will cease the related processing going forward.
- **Right to Grievance Redressal:** If you have any concerns or complaints regarding your personal data, you have the right to raise a grievance with us. We will acknowledge and resolve complaints within a reasonable time. If you are not satisfied with our response, you can escalate the complaint to the Data Protection Board of India, once it is operational.

- **Right to Nominate a Representative:** You may nominate, in writing, an authorized individual (e.g. a family member) to exercise your data rights on your behalf in case of your incapacity or death.

To exercise any of these rights, please contact us using the contact information below. We will need to verify your identity (or authority, if through a nominee) before fulfilling requests. We will respond to valid requests as soon as possible, within any timeframe required by law.

Contact Us and Grievance Officer [🔗](#)

If you have questions about this Privacy Policy or wish to contact us regarding your personal data, please reach out to contact below:

- **Name:** Rishabh Agrahari, CEO and Founder
- **Email:** agrahari@sanch.ai
- **Postal Address:** Rishabh Agrahari, Sanchai Analytics Pvt. Ltd., D11, Supriya Garden, Nagras Rd, Aundh Pune, Maharashtra, India.

This person is responsible for addressing user grievances and overseeing compliance with this policy. Under the DPDP Act, you can expect a resolution or update on any grievance within two weeks. If you are not satisfied with the resolution of your complaint, you may lodge a complaint with the Data Protection Board of India.

Updates to this Policy: We may update this Privacy Policy from time to time to reflect changes in our practices or legal obligations. Material changes will be communicated via our website or through direct notification. The "Effective Date" at the top will always indicate when the latest changes were made. We encourage you to review this Policy periodically.