

Policy for Digital Personal Information and Data Protection

1. Introduction

The right to privacy is a fundamental right and is necessary to protect personal data as an essential facet of information privacy. The growth of the digital economy has meant the use of the data as a critical means of communication between people. Hence it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the information privacy of individuals, and ensuring empowerment, progress and innovation.

Our Information Security Philosophy is to ensure that the right data is used by a person in the right role and only in the right context, so that internal and external customers and other stakeholders can trust us for their business. Our Data Privacy Policy is a legal document that we use to disclose the way we gather, use and manage the personal information of our customers, clients and employees. Personal information can be anything that identifies an individual. Our Data Privacy Policy not only covers our customers but also covers our business partners, suppliers and employees.

We follow strict security procedures in the storage and disclosure of any information so that our internal and external clients, employees, Board members, other partner in our organization (voluntary or otherwise), contractor or agent feel confident about the privacy and security of their personal information.

We handle data protection and privacy by categorizing all data based on our sensitivity (confidentiality), criticality (availability), identifiability (privacy) and compliancy; this categorization is then used to determine the safeguards required.

Our Company's Data Protection Policy refers to our commitment to treat information of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality. With this policy, we ensure that we gather, store and handle data fairly, transparently and with respect towards individual rights.

2. Definition

Personal data: Any information that directly or indirectly identifies an individual.

Data Controller: A person, department or organisation that determines the purpose and means of data processing.

Data Subject: An individual whose personal data is subject to processing

Processing: Any operation or set of operations applied to Personal Data, such as data collection, recording, organization, structuring, storage, adaptation, modification, extraction, consultation, use and transmission.

3. Who is covered under the Data Protection Policy?

Employees, apprentice, of our Company and subsidiaries or entities under the same group, must follow this policy. Contractors, consultants, partners and any other external entity are also covered. Generally, our policy refers to anyone we collaborate with or acts on our behalf and may need occasional access to data.

4. Policy elements

As part of our operations, we need to obtain and process information of customer or vendors or consultants or employees. This information includes any offline or online data that makes a person identifiable such as names, addresses, usernames and passwords, digital footprints, photographs, social security numbers, financial data etc., KYC documents.

Our company collects this information in a transparent way and only with the full co-operation and knowledge of interested parties. Once this information is available to us, the following rules apply.

4.1 Our data will be:

- Accurate and kept up-to-date;
- Collected fairly and for lawful purposes only;
- Processed by the Company within its legal and moral boundaries;
- Protected against any unauthorized or illegal access by internal or external parties;
- To carry out processing of personal data in a transparent manner;

4.2 Our data will not be:

- Communicated informally;
- Stored for more than a specified amount of time;
- Transferred to organizations, states or countries that do not have adequate data protection policies;
- Distributed to any party other than the ones agreed upon by the data's owner (exempting legitimate requests from law enforcement authorities);

In addition to the ways of handling the data, Company has direct obligations towards people to whom the data belongs. Specifically, we must:

- Let people know which of their data is collected;
- Inform people about how we will process their data;
- Inform people about who has access to their information;
- Have provisions in cases of lost, corrupted or compromised data;
- Allow people to request that we modify, erase, reduce or correct data contained in our databases.

4.3 How we collect personal data

We are committed to collect personal data through lawful and transparent means, with your explicit consent where required, which include:

- When you provide information to us by filling in the forms on our website or offline;
- When you contact us, for example, to enquire about our services or apply for a job or face to face;
- Through our provision of services to you, or the organization you represent;
- Sending us a letter, e-mail or social media message;
- Requesting promotional information from us (e.g. information about any of our products or services) participating in a survey, competition or prize draw;

4.4 How we use your personal information:

We have a legitimate business interest in operating and improving its business and the services we offer and therefore we use and processes personal data, and we will not do so to the extent that processing would override customers', vendors, consultants or employees' interests, rights and freedoms to protect their personal data. In this situation, we shall only process their personal data they have given us their explicit consent, and they have the right to withdraw their consent at any time.

We process personal information for the following purposes:

- For research, planning, service development, security or risk management;
- To carry out services we have agreed to provide;
- To comply with legal and professional obligations;

4.5 Prevention, detection, investigation and prosecution of contraventions of law

Processing of personal data in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law shall not be permitted unless it is authorized by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests being achieved.

4.6 Actions

To exercise data protection, we are committed to:

- Restrict and monitor access to sensitive data;
- Develop transparent data collection procedures;
- Train employees in online privacy and security measures;
- Build secure networks to protect online data from cyber-attacks;
- Establish clear procedures for reporting privacy breaches or data misuse;
- Include contract clauses or communicate statements on how we handle data;

- Establish data protection practices (document shredding, secure locks, data encryption, frequent backups, access authorization etc.);

5. Dissemination of the policy

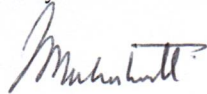
Our Company's Data protection policy will be updated on Company's official website and shall be part of the Company's policy document.

6. Amendment

The Board reserve the power to review and amend this policy from time to time. This policy would be subject to revision/ amendment in accordance with applicable laws as may be issued by the relevant statutory government and regulatory authorities, from time to time. In case any amendment(s), clarification(s), circular(s) etc. issued by the relevant statutory, governmental and regulatory authorities are not consistent with the provisions laid down under this Policy, then such amendment(s) clarification(s), circular(s) etc., shall prevail upon the provisions hereunder.

This policy is adopted by the Board of Directors in its meeting held on **March 10, 2026**.

For Online Instruments (India) Limited
(Formerly Online Instruments (India) Private Limited)



~~Shivanand Mallappa Mahashetti~~
Managing Director
DIN: 01180544

For Online Instruments (India) Limited

Authorised Signatory