Trust Fintech Limited

PRIVACY POLICY

1. OBJECTIVES:

The purpose of this Privacy Policy is to establish TFL's commitment to protecting the privacy, confidentiality, and integrity of all personal and sensitive personal data processed within the organization.
It ensures compliance with applicable data protection and information security regulations including **ISO/IEC 27001:2022**, **ISO/IEC 27701:2019 (Privacy Information Management)**, and **relevant legal frameworks such as the Information Technology Act, 2000 and CERT-In Directions (2022)**.
• Ensure privacy by design and by default in all business processes and systems.
• Enable transparency and accountability in how personal information is collected, stored, used, and shared.

2. SCOPE:

This policy applies to:

- All personal and sensitive personal data collected, processed, stored, or transmitted by the organization in any form — electronic, physical, or cloud-based.
- All employees, contractors, consultants, vendors, and third parties who have access to or process such data.
- All business functions (e.g., HR, Finance, IT, Operations, Sales) where personal data is handled.
- This policy applies equally to subsidiaries, joint ventures, and cloud environments where the organization is the data controller or processor.
- Visitors, customers, and other data subjects interacting with organizational systems are also covered.
-

3. DEFINITIONS:

Term	Definition
Personal Data	Any information that can identify an individual (e.g., name, contact details)
Sensitive Personal Data	Financial information, passwords, biometrics, health records, etc.
Data Subject	The individual whose personal data is being collected or processed
Data Controller	The organization that determines the purpose and means of data processing
Data Processor	A third party processing data on behalf of the organization
Data Protection Officer (DPO)	The designated officer responsible for overseeing privacy compliance and handling data subject requests.
Consent	Freely given, informed, and explicit indication of the data subject's agreement to process their data.

.

CONTROL REFERENCE NUMBERS:

Standard / Framework	Control Reference
ISO/IEC 27001:2022	A.5.10, A.8.11, A.8.12, A.8.15
ISO/IEC 27701:2019	7.2.1 – 7.5.9
CERT-In Directions (2022)	Section 4 – Data Retention & Incident Reporting
IT Act 2000 / SPDI Rules 2011	Rule 3 & 5

5. POLICY DETAILS:

- **Principles of Privacy (Aligned with ISO 27001 & Legal Standards)**
  The organization commits to processing personal data in accordance with the following principles:

  - **Lawfulness, Fairness, and Transparency**
    Data must be collected lawfully and with clear communication to the data subject.
  - **Purpose Limitation**
    Data must only be collected for specific, legitimate purposes and not used beyond those.
  - **Data Minimization**
    Only the data necessary to perform the task should be collected.
  - **Accuracy and Relevance**
    Data must be accurate and kept up to date and relevant for any requirements.
  - **Storage Limitation**
    Data should be retained only as long as necessary (see Retention section).
  - **Integrity and Confidentiality**
    Personal data must be protected against unauthorized access, alteration, and loss.
  - **Accountability and Auditability**
    All employees must follow this policy and demonstrate compliance.

- **Data Collection and Usage**
  - Personal data may be collected for purposes such as:
  - GST system registration and compliance
  - Employee records and payroll
  - Vendor or contractor management
  - Customer support and inquiries
  - Where required, **consent** will be obtained before data collection.
  - Data shall be collected only for legitimate business or regulatory purposes and with prior consent where applicable.
  - Data subjects shall be informed of the collection purpose, retention duration, and their rights.

- **Access Control and Protection**
    - Access to personal data is role-based and limited to authorized personnel only.
    - All systems handling personal data are secured using encryption, firewalls, and strong authentication.
    - Logs are maintained to track access and modifications.
    - Role-based access controls, encryption (AES-256), and secure transmission (TLS 1.2+) shall be enforced.
    - All personal data stored in systems shall be regularly backed up and monitored for unauthorized access.

- **Data Sharing and Third Parties**
    - Personal data may be shared with:
    - Government agencies (e.g., GSTN, CERT-In) under legal obligations
    - Third-party processors (under strict contractual terms)
    - Data will never be sold or shared without legal or business justification.
    - Third-party data processors must sign a Data Processing Agreement (DPA) defining confidentiality, security, and retention obligations.
    - Data sharing across borders must comply with applicable data export laws and organizational approval procedures.

- **Data Retention and Disposal**
    - Retention periods must be defined in line with legal or business requirements (minimum 2 years or as mandated).
    - After expiry, data must be securely destroyed using approved methods such as wiping, shredding, or cryptographic erasure.

- **Rights of Data Subjects**
    - Individuals have the right to:
        - Data subjects may **request access, correction, deletion, or withdrawal of consent at any time** (if applicable).
        - Report privacy violations
        - Requests can be directed to contact email or DPO
        - All verified requests shall be fulfilled within 30 days.
        - Requests are to be logged in the Data Subject Request Register managed by the DPO.

- **Incident Management**
    - All suspected or confirmed data privacy incidents (e.g., data breach or unauthorized access) must be reported immediately to the **Security Incident Response Process**, DPO or Security Team.
    - Incidents will be logged, investigated, and reported to bodies as required.
    - Incident response must include containment, investigation, root-cause analysis, and notification to authorities where required.

  - **Information Security Incident Response Policy** must be followed for breach handling.

- **Training and Awareness**
  - All employees must undergo **annual training** on data privacy and security practices. Special roles (e.g., HR, IT, finance) may require more frequent or advanced training.
  - Departments processing sensitive data shall undergo quarterly refresher training.
  - Maintain attendance and training records for compliance audits.

6. ROLES AND RESPONSIBILITIES:

Role	Responsibility
Data Protection Officer (DPO)	Oversee compliance with privacy laws, handle data subject requests, and report breaches.
Information Security Team	Ensure implementation of security controls protecting personal data.
Department Heads	Enforce policy within their functions and ensure lawful data collection.
Employees / Users	Handle personal data responsibly and report any suspected data misuse.
Vendors / Third-Party Processors	They must comply contractually with this policy.

7. COMPLIANCE AND MONITORING:

• Periodic privacy audits shall be conducted to ensure adherence to this policy and regulatory requirements.

• External audits may be carried out annually to validate ISO 27701 compliance.

Non-compliance with this policy may result in:

- Disciplinary action
- Legal penalties
- Regulatory reporting obligations

8. POLICY REVIEW AND UPDATE:

This policy will be:

- Reviewed annually, or upon significant regulatory or business changes.

- Updated based on audit findings, data protection impact assessments (DPIA), or new technologies.
- The latest approved version shall be published internally and made available to relevant stakeholders.

9. REFERENCES:

SN	Title / Source	Reference Description
1	ISO/IEC 27001:2022 – Information Security Management Systems	Defines controls for secure handling and protection of information.
2	ISO/IEC 27701:2019 – Privacy Information Management System	**Extends ISO 27001:2022** with privacy-specific controls for personal data protection.
3	IT Act 2000 & SPDI Rules 2011 (India)	Establishes legal framework for handling personal and sensitive personal data.
4	CERT-In Directions (2022)	Provides directives for log retention, breach reporting, and cybersecurity governance.
5	NIST SP 800-122 – Guide to Protecting the Confidentiality of PII	Reference for global best practices in protecting personal information.