TechFino Capital Private Limited

Privacy Policy

Doc. No.	TCPL-ISMS-PL-25
Issue No. & Date	Ver 2.0 – 07-11-2025
Classification of Information	Internal and Protected

Table of Contents

1. Purpose

The purpose of this Policy is to protect personal information (including personally identifiable information or PII) and sensitive personal data or information (SPDI), by putting in place appropriate controls across the organization, periodically reviewing them and improving them as needed.

The organization ensures compliance with the relevant legal requirements and contractual requirements from customers related to privacy, including:

- The Digital Lending Guidelines issued by the Reserve Bank of India (RBI)
- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules")
- The Digital Personal Data Protection Act, 2023 and related regulations
- RBI guidelines on digital lending, outsourcing, and data storage
- Credit bureau regulations and sectoral data protection requirements
- All applicable local, state, and central government regulations regarding cross-border data transfers

2. Scope

The scope of this policy includes:

- All employees of TCPL and those of our business associates who have or are responsible for the collection, use, retention, disclosure, and disposal of personal information and sensitive personal data
- All personal information and sensitive personal data or information collected by TCPL or its affiliates directly from customers through TCPL's online portals, electronic communications, or through business processes
- All cross-border data flows and international data transfers
- All third-party service providers, vendors, and outsourcing partners involved in data processing

3. Roles & Responsibilities

Roles	Responsibilities
Chief Information Security Officer (CISO)	• Approve all mandatory documents and compliance policies • Oversight of data protection and privacy compliance • Approval & communication with Authority and Regulatory Bodies • Ensure cross-border data transfer compliance framework is in place
Compliance Officer / Legal Team	• Maintain regulatory watch for notifications under Section 16 of the Digital Personal Data Protection Act, 2023 • Monitor updates from MeitY, RBI, and the Data Protection Board

	• Maintain and update inventory of cross-border data flows • Review and approve all new cross-border data transfers and third-party services • Coordinate sector-specific regulatory compliance assessments
Head of IT/Infrastructure	• Implement technical controls for data security • Manage vendor relationships and ensure data localization requirements • Maintain alternative data storage solutions within approved jurisdictions • Respond immediately to restricted country notifications
Head HR	• Document, Communicate, and ensure implementation and maintenance of this policy • Conduct staff awareness training on cross-border data transfer restrictions • Ensure all staff understand data handling requirements

4. Abbreviations & Definitions

4.1 Abbreviations

Abbreviation	Expansion
TCPL	TechFino Capital Private Limited
DPDP Act	Digital Personal Data Protection Act, 2023
SPDI Rules	Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
RBI	Reserve Bank of India
MeitY	Ministry of Electronics and Information Technology
DLG	Digital Lending Guidelines (RBI)
PII	Personally Identifiable Information
SPDI	Sensitive Personal Data or Information
MLI	Member Lending Institutions
CISO	Chief Information Security Officer
SaaS	Software as a Service

4.2 Definitions

Terms	Definitions
Personal Information	Any information that relates to a natural person, either directly or indirectly, in combination with other information available or likely to be available with TCPL, is capable of identifying such a person. This includes name, email, contact

	details, address, designation, credit information, and any other identifiable data.
Sensitive Personal Data or Information (SPDI)	As defined under Rule 3 of the SPDI Rules, 2011, this includes: passwords; financial information such as bank account, credit card, debit card details; physical, physiological and mental health condition; sexual orientation; medical records and history; biometric information; genetic information; trading and financial history; any information provided with an explicit purpose of not being further shared.
Consent	Voluntary, informed, and unambiguous agreement by the data subject to the collection, processing, use, and disclosure of their personal information or SPDI. Consent must be explicit, prior, and obtained through a click-wrap mechanism with documented audit trail.
Click-Wrap Mechanism	An electronic consent method where the user must actively click "I Agree," "Accept," or similar action to confirm understanding and acceptance of terms before data is collected or processed. The system must record timestamp, user action, and IP address to create an electronic audit trail.
Cross-Border Data Transfer	Movement of personal information or SPDI from India to any country outside India, whether through cloud storage, SaaS platforms, outsourcing partnerships, international offices, or any other means.
Restricted Country	Any country or jurisdiction that has been notified by the Central Government of India as prohibited for personal data transfers under Section 16 of the DPDP Act, 2023.
Data Localization	The requirement or practice of maintaining personal information or SPDI within a specific geographic jurisdiction, typically India, as mandated by applicable laws or regulations.

5. Forms

Name of the Document	**Form No.**

6. Policy

TCPL recognizes the expectations of its customers with regard to privacy, confidentiality, and security of their personal information that resides with the organization.

TCPL is working with Member Lending Institutions (MLIs), which are in the banking and financial services industry and registered with TCPL under various credit guarantee schemes. Keeping the personal information of borrowers secure, using collected information solely for legitimate business and data validation purposes, and preventing any misuse of information is a top priority for TCPL.

TCPL has adopted a comprehensive privacy policy aimed at protecting the personal information of borrowers and other data subjects entrusted and disclosed by the Member Lending Institutions (MLIs) and other business partners.

Privacy Policy governs the way in which the organization:

- Collects personal information and sensitive personal data
- Uses, discloses, stores, and secures such information
- Manages cross-border transfers in compliance with Section 16 of the DPDP Act and RBI guidelines
- Disposes of personal information at end of retention period
- Ensures compliance with Digital Lending Guidelines, particularly Paragraphs 10 and 12

TCPL commits to:

- Obtain explicit, prior consent through click-wrap mechanisms for all data collection and processing
- Maintain transparency in all data handling activities
- Respect the rights of data subjects to access, rectify, delete, and port their data
- Implement robust security controls in line with ISO 27001:2022
- Comply with all sector-specific regulations, particularly RBI guidelines on digital lending and data localization
- Regularly audit and update cross-border data transfer practices

7. Information We Collect

We collect only the information needed for legitimate business purposes, in strict compliance with the Digital Lending Guidelines and SPDI Rules.

7.1 Personal Information

You may need to provide personal information such as:

- Full name
- Email ID and contact details (phone, mobile)
- Residential and correspondence address
- Designation and employment details
- Credit information and financial history
- Borrower identification details
- Unique identification numbers (as applicable)

7.2 Sensitive Personal Data or Information (SPDI)

When applicable and with explicit consent, we may collect:

- Financial information (bank account details, credit card, debit card numbers)
- Medical records and health-related information
- Biometric information (fingerprints, iris scans, as per applicable regulations)
- Physical, physiological, and mental health status
- Genetic information
- Trading history and financial performance data
- Passwords and security credentials

7.3 Collection Methods

We may collect personal information:

- Directly from you when you sign up, register, request services, or provide information voluntarily
- Through your employer or Member Lending Institutions (MLIs)
- From publicly available databases (where permitted by law)
- From third-party partners with whom you have authorized information sharing
- Through analytical tools and cookies on our digital platforms

8. Consent & Data Collection Framework

8.1 Explicit Consent Requirement

TCPL will obtain explicit, prior written consent from all data subjects before collecting, processing, or sharing any personal information or SPDI. Consent shall be:

- Voluntary: Not coerced or obtained under duress
- Informed: Data subject must understand the purpose, scope, and implications of data collection
- Specific: Clearly delineated for each purpose of collection and processing
- Unambiguous: Expressed through a clear affirmative action

8.2 Click-Wrap Consent Mechanism (Rule 5(1) - SPDI Rules, 2011)

All consent for personal information and SPDI collection shall be obtained through an electronic click-wrap mechanism in compliance with Rule 5(1) of the SPDI Rules, 2011. The mechanism shall include:

Mandatory Elements:

1. Clear and Conspicuous Notice: Before any data collection, a prominent notice must display: the purpose of data collection; type of data being collected; intended use and sharing of data; duration of data retention; rights of the data subject.

2. Active Opt-In: The data subject must actively click "I Agree," "Accept," "Confirm," or similar button to signify consent. Pre-checked boxes are NOT permitted.

3. Audit Trail: The system must automatically record and maintain: timestamp of consent; IP address of data subject; unique identifier or email of consenting party; version of consent terms accepted; method of consent (click-wrap); any modifications to consent.

4. Accessibility: Consent forms must be: in plain, understandable language; available in multiple languages (English, Hindi, and local languages as applicable); accessible for persons with disabilities; easily printable and downloadable.

5. Separate Consents: Different purposes shall have separate consent forms: consent for collection of general personal information; separate consent for collection of SPDI; separate consent for data sharing with third parties; separate consent for cross-border data transfers; separate consent for marketing or analytics purposes.

6. Revocation: Data subjects must be able to withdraw consent at any time by submitting a request to admin@techfino.in. TCPL will cease processing within 5 business days of consent withdrawal.

8.3 Consent for Third-Party Sharing

Before sharing personal information or SPDI with any third party, TCPL shall:

- Obtain specific written consent from the data subject
- Disclose the identity of the third party or category of third parties
- Explain the purpose of sharing
- Specify what data will be shared
- Allow data subjects to refuse sharing without affecting their ability to use TCPL services

9. Digital Lending Guidelines Compliance

TCPL ensures compliance with RBI's Digital Lending Guidelines through:

Data Collection Standards:

- Collection of personal and financial information is strictly need-based
- Data collection is limited to information essential for credit assessment, loan origination, and regulatory compliance
- No excessive or unnecessary data is collected
- Data subjects are explicitly informed of the business purpose for each data element requested

Purpose Limitation:

- Personal information is used solely for the purpose for which it was collected
- Any use beyond the original purpose requires fresh, explicit consent
- TCPL shall not reuse data for unrelated purposes without obtaining separate consent
- All uses of data for analytics, marketing, or secondary purposes require explicit consent

Third-Party Sharing Controls:

- Personal information is not shared with third parties without explicit, prior consent from the data subject
- In cases where sharing is legally mandated (by RBI, credit bureau regulations, statutory requirements), TCPL will inform the data subject of such mandated sharing
- Credit bureau sharing is limited to information required for credit reporting purposes only
- No data is shared for promotional, marketing, or non-essential third-party purposes without clear data subject consent

Borrower Empowerment:

- TCPL provides borrowers with clear information about who has access to their data
- Borrowers can request to know all third parties with whom their data is shared
- Borrowers can restrict data sharing (where legally permissible)
- Borrowers can view an audit log of all data access and sharing events related to their account
- Borrowers can trigger data erasure and removal from TCPL systems upon request, subject to legal retention requirements

Transparency in Data Practices:

- This Privacy Policy clearly outlines all data handling practices
- Data subjects receive clear disclosure of how their data will be used, shared, stored, and protected
- TCPL maintains a data register documenting all data collection, processing, and sharing activities
- Regular transparency reports are prepared for regulatory authorities upon request

Accountability Mechanisms:

- A dedicated compliance team oversees all data handling activities
- Regular internal audits are conducted to ensure compliance with this policy and applicable laws
- An audit trail is maintained for all data access, processing, and sharing
- Senior management reviews data handling practices quarterly
- Non-compliance is escalated to the CISO and compliance officer immediately

Grievance Redressal:

- Data subjects can submit privacy complaints to admin@techfino.in
- Complaints are acknowledged within 5 business days
- TCPL commits to resolving complaints within 30 days
- Data subjects can approach the RBI or competent authorities if not satisfied with TCPL's response

10. What We Do With Your Personal Information

10.1 Purpose of Use

We use personal information and SPDI solely for the specific purposes for which it is provided and for compatible purposes that data subjects would reasonably expect. These purposes include:

Legitimate Business Purposes:

- Credit assessment and loan underwriting
- Loan disbursement and repayment management
- Regulatory compliance and reporting to RBI and credit bureaus
- Identity verification and KYC (Know Your Customer) requirements
- Fraud prevention and detection
- Customer service and support
- Updating records and maintaining accurate customer information

Essential Operational Purposes:

- To manage, administer, and fulfill obligations under contracts with borrowers and Member Lending Institutions (MLIs)
- To comply with legal and regulatory requirements from government, RBI, courts, or other authorities
- To maintain records for audit and compliance purposes
- To prevent or detect unauthorized access or fraud

Analytical & Improvement (Only With Explicit Consent):

- Analyzing trends in borrower data for business intelligence (only with separate consent)
- Improving our services and user experience (only with separate consent)
- Conducting research on lending practices and market trends (only with anonymized/pseudonymized data)

11. Data Sharing & Third-Party Disclosures

11.1 Non-Sharing Commitment

TCPL commits to the following principles regarding data sharing:

- We do NOT share or sell personal data to any third party except as explicitly permitted in this policy
- We do NOT monetize personal data through marketing, advertising, or broker arrangements
- We do NOT transfer personal data to data brokers or commercial entities for commercial gain

11.2 Permitted Data Sharing

Personal information or SPDI may be shared with third parties only in the following circumstances:

1. With Explicit Data Subject Consent

TCPL provides the data subject with clear disclosure of: the identity or category of third parties; the purpose of sharing; what specific data will be shared; duration of access by third parties. Data subjects can refuse sharing without penalizing their access to TCPL services.

2. With Legally Required Disclosures

- Reserve Bank of India (RBI): Loan data, borrower information, and compliance reports as required by Digital Lending Guidelines

- Credit Bureaus: Credit history and repayment information (limited to purposes specified in credit bureau regulations)
- Government Agencies: Tax authorities, law enforcement, or other government bodies acting under legal authority
- Courts & Judicial Orders: Response to court orders, legal summons, or judicial directives
- Regulatory Authorities: Data Protection Board, Ministry of Electronics & Information Technology (MeitY), or other regulatory bodies
- Financial Intelligence Unit (FIU): Suspicious transaction reports and anti-money laundering (AML) compliance

12. Cross-Border Data Transfer Compliance

TCPL shall comply with all restrictions on cross-border data transfers as mandated by the Central Government under the DPDP Act, 2023. All personal data transfers to foreign jurisdictions are subject to government notification and approval.

12.2 Regulatory Watch - Monitoring Restricted Countries

Designated Responsibility:

The Compliance Officer or Legal Team is assigned responsibility for monitoring all notifications and updates regarding cross-border data transfer restrictions. This function shall be treated as a critical compliance activity.

Monitoring Mechanisms:

- Primary Source: Regular checking of official government notifications from MeitY, Data Protection Board, RBI, and Department of Telecommunications
- Secondary Sources: Industry associations (ASSOCHAM, FICCI, CII, NASSCOM, fintech consortiums), legal and compliance forums, regulatory newsletters
- Frequency: Monthly review of regulatory updates; immediate escalation if a new restriction is announced
- Documentation: Maintain a register of all restricted countries and the date of notification

12.3 Inventory of Cross-Border Data Flows

TCPL shall conduct and maintain a comprehensive inventory of all cross-border data flows. This inventory shall document:

- Type of personal data being transferred (customer data, financial data, operational data)
- Volume (number of records, size in GB) and frequency of transfers
- Cloud service provider name and country of server location
- SaaS applications and their data storage countries
- International offices or subsidiaries accessing TCPL data
- Outsourcing vendors with international presence and countries involved

12.4 Contingency Plans for Restricted Countries

TCPL shall develop and maintain contingency plans for each cross-border data dependency identified in the inventory. These plans ensure rapid response if a country is declared restricted.

Contingency Plan Components:

- Risk Assessment: Identify operational, business, and regulatory implications if data transfer to that country is blocked
- Alternative Solutions: Identify Indian-based service providers, approved country alternatives, or hybrid approaches
- Vendor Contract Clauses: All vendor agreements must include data relocation clauses, exit clauses, compliance clauses, and termination clauses
- Transition Timeline: Days 0-2: Immediate escalation; Days 2-5: Assess impact; Days 5-15: Execute data migration; Days 15-30: Complete transition
- Communication Plan: Notify internal stakeholders, MLIs, customers, and regulatory authorities

12.5 Data Flow Governance in Procurement & Projects

All procurement activities and new project initiations must include a data flow assessment before vendor selection or tool deployment.

Procurement Checklist - Cross-Border Data Transfer Questions:

1. Does this vendor/tool/service involve any data transfer outside India?
2. What countries are involved in data processing or storage?
3. Are all identified countries currently approved for data transfers under Section 16 of the DPDP Act?
4. What type of data is transferred?
5. Is explicit data subject consent in place for this cross-border transfer?
6. Has a Data Processing Agreement (DPA) been executed with the vendor?
7. Is this a regulatory compliance requirement (RBI, credit bureau, etc.)?

Approval Authority: Compliance Officer must sign off on data flow before procurement is finalized. No vendor/tool/service involving cross-border data can be deployed without compliance approval.

12.6 Internal Policy Statement on Cross-Border Transfers

TCPL Cross-Border Data Transfer Policy:

TCPL will not transfer personal data, sensitive personal data or information, or any other regulated data of its customers, borrowers, or data subjects to any country prohibited by the Central Government of India for such transfers under Section 16 of the Digital Personal Data Protection Act, 2023.

TCPL will strictly comply with all conditions prescribed by the Central Government if any are specified for transfers to certain jurisdictions.

All cross-border data transfers are pre-approved by the Compliance Officer and monitored continuously. If a country is declared restricted, TCPL will immediately suspend data transfers and migrate data to an approved jurisdiction within 30 days.

Employees, contractors, and vendors are prohibited from transferring personal data to any foreign jurisdiction without explicit compliance approval. Violations of this policy will result in disciplinary action, including termination of employment or contract.

Staff Awareness:

All employees, contractors, and relevant third parties shall be provided with annual training on cross-border data transfer restrictions, clear examples of prohibited practices, escalation procedures, and consequences of non-compliance.

12.7 Immediate Response Mechanism for Restricted Country Notifications

Upon receipt of a government notification that a country is restricted for data transfers:

- Immediate Actions (Within 2 Hours): Compliance Officer verifies notification; CISO is informed; emergency meeting convened
- Identification Phase (By End of Day 1): Cross-reference restricted country with data flow inventory; identify all affected vendors and services
- Escalation (By Day 2): Notify all stakeholders; instruct vendors to cease transfers; activate alternative solutions
- Mitigation (Days 2-30): Execute contingency plan; migrate all data to approved jurisdiction; terminate non-compliant agreements
- Communication & Compliance (Day 30 Onwards): Verify complete relocation; file compliance certification with RBI; update privacy policy and inventory

13. Sector-Specific Data Transfer & Localization Regulations

13.1 Identification of Applicable Sector-Specific Regulations

Beyond the general DPDP Act, 2023, TCPL is subject to sector-specific data protection and localization regulations. These include:

RBI Regulations for Digital Lending & Fintech:

- Digital Lending Guidelines (2022, updated 2025): Specify data collection standards, borrower consent requirements, and outsourcing norms
- RBI Outsourcing Guidelines: Require data to be outsourced only to approved locations with specific security and confidentiality requirements
- Credit Information Policy: Specify how credit data can be collected, stored, shared, and used
- Payment System Regulations: Require payment-related data to be stored and processed within India

Credit Bureau Regulations:

Credit information collected by credit bureaus must be: used only for credit reporting and scoring purposes; stored and processed in compliance with credit bureau license requirements; not shared with third parties without explicit consent; typically stored within India or in approved jurisdictions.

Other Applicable Regulations:

- Aadhaar Act, 2016: Aadhaar data cannot be transferred outside India or used for unauthorized purposes
- Telecom Regulations: If TCPL handles telecom data, it must comply with TRAI regulations on data localization
- Payment Card Industry Data Security Standard (PCI-DSS): If handling card data, must comply with international standards (while localizing sensitive data)
- Employment Data: Employee data must be protected under Employment Codes and cannot be arbitrarily transferred

13.2 Gap Analysis - Current Practices vs. Regulatory Requirements

TCPL shall conduct a gap analysis by comparing current data handling practices against all applicable sectoral regulations.

Gap Analysis Process:

- List All Systems & Processes: Document all systems handling data and their locations (India/Foreign)
- Cross-Reference Regulatory Requirements: For each system, identify applicable regulations
- Identify Gaps: Compare actual vs. required practices
- Remediation Plan: For each gap, document immediate actions, timeline, responsible party, and resources
- Documentation: Maintain a Gap Analysis Register documenting each identified gap, regulatory basis, severity, timeline, and status

13.3 Explicit Compliance Statements

TCPL Internal Policy on Sectoral Compliance:

TCPL recognizes that in addition to general data protection laws such as the DPDP Act, 2023, the company is subject to sector-specific regulations issued by the Reserve Bank of India, credit bureau regulators, and other authorities.

The company commits to:

1. *Comply with RBI's Digital Lending Guidelines on data collection, borrower consent, data storage, and third-party sharing*
2. *Comply with RBI's Outsourcing Guidelines on approved jurisdictions and vendor confidentiality*
3. *Comply with Credit Bureau Regulations on India-only storage and limited use of credit data*
4. *Comply with Other Applicable Laws including Aadhaar Act, Telecom Regulations, Employment Laws, and Income Tax Laws*

5. *Hierarchy of Compliance: In case of conflicting requirements, TCPL will comply with the strictest requirement*
6. *Regular Review & Update: TCPL will review these policies annually or upon receipt of new regulatory guidance*
7. *Enforcement: Violations will result in disciplinary action for employees and termination of contracts for vendors*

13.4 Coordination with Legal & Compliance Teams

Whenever TCPL considers a new service, vendor, tool, or process that involves cross-border data handling, the following approval process is mandatory:

- Step 1 - Business Request (Day 0): Department submits Cross-Border Data Request Form to Compliance Officer
- Step 2 - Compliance Review (Days 1-3): Compliance Officer assesses country approval, data type, sector-specific restrictions, and consent requirements
- Step 3 - Legal Due Diligence (Days 3-7): Legal Team evaluates vendor terms, Indian law compliance, and security adequacy
- Step 4 - Approval or Rejection (Day 7): If compliant, approved; if non-compliant, rejected with alternatives proposed
- Step 5 - Contract & DPA (Days 7-14): Vendor contract must include data localization clauses and Data Processing Agreement
- Step 6 - Implementation (Day 14+): Tool/vendor deployed only after contract execution, DPA signing, inventory update, and training

13.5 Examples & Staff Awareness

TCPL Sector-Specific Data Protection Training - Key Points. All staff shall be aware of the following examples:

Example 1 - Payments Data: Payments-related data must stay in India due to RBI regulations. If your department uses an international payment processor, ensure they process and store data only in Indian data centers. Violation could result in RBI penalties.

Example 2 - Aadhaar Information: Do not send Aadhaar information to any foreign system. Aadhaar data cannot leave India under the Aadhaar Act. Transferring Aadhaar abroad is a criminal offense.

Example 3 - Credit Information: Borrowers' credit data cannot be shared or stored outside India. If TCPL uses credit bureau services, ensure credit data stays in India.

Example 4 - Foreign Vendors & Outsourcing: If your department engages a foreign call center, BPO, or service provider to handle customer data, we must comply with RBI Outsourcing Guidelines. The vendor must be pre-approved by RBI or located in an approved jurisdiction.

Example 5 - New SaaS Tools: Before adopting a new cloud-based tool (CRM, analytics, HR system), check with the Compliance Officer whether the tool stores data in an approved country. Ensure the

country is approved under Section 16, no sector-specific regulation prohibits storage, a Data Processing Agreement is in place, and data subject consent is obtained. Do not deploy without compliance sign-off.

Example 6 - Personal Data vs. SPDI: Different data requires different protections. Financial data must stay in India (per RBI rules). Aadhaar data cannot go abroad (per Aadhaar Act). Health data requires explicit consent (per SPDI Rules). Always ask: Is this SPDI? If yes, apply stricter protections.

Training Documentation:

- Annual mandatory training on sector-specific data regulations
- Training records maintained for audit purposes
- Case studies and real-world examples discussed
- Quiz or assessment to verify understanding
- Refresher training when new regulations are issued

14. How Long Will We Keep Your Personal Information?

We will only retain your personal data for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

14.1 Retention Periods by Data Type

Customer & Borrower Data:

- Active Loan Period: Duration of the loan plus 7 years from the last transaction date (as per banking regulations)
- Closed Accounts: 7 years from closure (for regulatory compliance and dispute resolution)
- Credit Bureau Data: 7 years per credit bureau regulatory requirements

Sensitive Personal Data (SPDI):

- Financial Records: 7 years minimum (per income tax regulations)
- Health & Medical Data: As required by applicable healthcare regulations; minimum 5 years
- Biometric Data: Duration of use plus 3 years; earlier deletion if purpose is fulfilled

Employee Data:

- During Employment: Duration of employment
- Post-Employment: 5 years for compliance and reference purposes

Audit & Compliance Records:

- Consent Audit Trails: 5 years minimum
- Data Access Logs: 3 years minimum
- Security Incident Records: 7 years minimum
- Regulatory Correspondence: As required by RBI and other authorities

14.2 Data Anonymization & Pseudonymization

- Once the purpose of collection is fulfilled, personal data will be anonymized or pseudonymized where possible
- Anonymized data may be retained indefinitely for statistical and research purposes
- Anonymization shall be performed using industry-standard techniques ensuring irreversible identification

14.3 Data Deletion & Disposal

- Upon expiration of retention periods, personal data shall be securely deleted
- Deletion shall be performed using industry-standard data destruction methods (secure erasure, physical destruction of media)
- Backup copies shall be deleted within 3 months of data deletion from primary systems
- Deletion shall be certified and documented in the Data Deletion Register

14.4 Data Subject Right to Erasure

Data subjects can request deletion of their personal data at any time. Deletion requests shall be processed within 30 days. Exceptions: Data required by applicable laws (tax records, regulatory compliance); data necessary for ongoing contractual obligations; data subject disputes deletion. Even after deletion from active systems, anonymized residual copies in backups may be retained for compliance purposes.

15. Information Security Measures

15.1 General Security Commitments

TCPL is fully committed to information security and compliance with applicable regulations. We have implemented strong security controls for the protection of data through our Information Security Management System aligned with ISO 27001:2022.

15.2 Technical Security Controls

- Encryption in Transit: All data transmitted outside TCPL networks is encrypted using industry-standard protocols (TLS 1.2 or higher)
- Encryption at Rest: Sensitive personal data and SPDI are encrypted using AES-256 or equivalent encryption standards
- Access Controls: Data access is restricted based on role-based access control (RBAC) principles
- Authentication: Multi-factor authentication (MFA) is enforced for access to sensitive data systems
- Network Security: Firewalls, intrusion detection systems, and VPNs protect network perimeters
- Database Security: Database access is logged; unauthorized access attempts are monitored and alerted
- Data Masking: Non-production environments use masked or anonymized data

15.3 Organizational Security Controls

- Information Security Policy: Comprehensive ISMS policies govern data protection organization-wide

- Staff Training: All employees receive annual information security and data protection training
- Confidentiality Agreements: All employees and contractors sign confidentiality agreements
- Third-Party Risk Management: Vendors are assessed for information security compliance before engagement
- Incident Response Plan: Security incidents are logged, investigated, and remediated promptly
- Security Audits: Regular security audits and penetration testing are conducted

15.4 User Responsibilities

Though TCPL takes reasonable measures to protect assets against unauthorized access or attack, the Internet inherently is not fully secure. Users must also take responsibility for their data security: maintain the confidentiality of your User ID and Password; do not share credentials; use secure devices and networks; keep systems updated with security patches; report any suspected security breaches immediately to admin@techfino.in.

15.5 Incident Reporting & Response

If you suspect any security issues, incidents, or receive suspicious communications claiming to be from TCPL, email admin@techfino.in immediately. Do not click links or provide information to suspicious communications. Verify the sender's identity independently before responding.

16. How Are Cookies Used?

A cookie is a small piece of data stored on the user's computer by the web browser while browsing a website. We use cookies to improve the quality of our site and service and to try and make your browsing experience meaningful.

16.1 Types of Cookies

First-Party Cookies: Mostly necessary for the website to function correctly. Include session cookies for login, preferences, and browsing state. Users can manage first-party cookies through browser settings.

Third-Party Cookies: Used mainly for understanding website performance. Include analytics, user interaction tracking, and security monitoring. Third-party cookies require explicit user consent.

16.2 Cookie Management

- User Control: You can control the use of cookies through your browser settings
- Consent: Upon first visit, you will be asked to consent to non-essential cookies
- Consent Revocation: You can withdraw cookie consent at any time through browser preferences
- Cookie Disabling: If you choose to disable cookies, certain website features or functions may not work optimally

17. How to Contact Us?

If you have a privacy concern, complaint, question, or request regarding this privacy statement and our data practices, please contact us:

17.1 Contact Information

Email: admin@techfino.in

Mailing Address: TechFino Capital Private Limited [Address to be provided]

Response Timeline:

- Acknowledgment: Within 5 business days
- Resolution: Within 30 days for standard requests
- Complex matters: Within 60 days (with notification of delay)

17.2 Data Subject Rights

You have certain rights regarding your personal information. You may contact us to exercise any of the following rights:

Right to Access: Request a copy of all personal data we hold about you; understand what data is collected and how it's used

Right to Rectification: Request correction of inaccurate or incomplete personal data; update outdated information

Right to Erasure: Request deletion of your personal data (subject to legal retention requirements); right to be "forgotten" where legally applicable

Right to Data Portability: Request your personal data in a structured, standard format; transfer your data to another organization

Right to Opt-Out: Withdraw consent for specific purposes; opt-out from marketing communications, analytics, or other non-essential processing

Right to Restrict Processing: Request suspension of data processing for specific purposes; limit how your data is used

Withdrawal of Consent: Withdraw consent previously granted for data collection or processing; future processing will cease upon consent withdrawal

17.3 Processing Requests

Request Submission: Submit requests by email to admin@techfino.in. Include sufficient detail for identification. Clearly state which right you wish to exercise.

Verification: You will be asked to verify your identity prior to processing the request. Verification ensures we disclose data only to the rightful data subject.

Approval or Denial: Requests will be processed on merit. If we cannot fulfill a request, you will be informed of the reasons.

Residual Copies: We may need to maintain residual copies of deleted data in backup systems for a limited period. Backup copies are deleted within 3 months of the primary deletion.

18. Legal Notice

18.1 Regulatory Disclosures

TCPL may need to disclose personal information to legal authorities for:

- Compliance with court orders, legal summons, or judicial directives
- Fraud investigation and prevention
- Statutory obligations under laws like RBI regulations, Income Tax Act, Prevention of Money Laundering Act (PMLA), and emergency response requests
- Data Protection Board inquiries

18.2 Confidentiality of Mandated Disclosures

Where legally required, TCPL shall: disclose information only to the extent legally mandated; attempt to notify the data subject of mandated disclosures (where not prohibited by law); maintain records of all disclosures for audit purposes; seek narrowing of disclosure requests where appropriate.

18.3 No Waiver of Rights

Providing this privacy policy does not constitute a waiver of any legal rights of TCPL or data subjects. TCPL reserves all legal rights to protect its interests and enforce its policies.

19. Changes to This Privacy Statement

We reserve the right to update this privacy policy at any time to: reflect changes in applicable laws and regulations; implement new data protection practices; respond to sector-specific regulatory updates (RBI guidelines, etc.); improve clarity or transparency of our privacy practices.

19.1 Notice of Changes

Substantial updates will be communicated to data subjects through: email notifications; website announcements; updates in user account portals. Significant changes will require re-confirmation of consent.

19.2 Effective Date

Changes become effective upon publication. Continued use of TCPL services after changes indicates acceptance of the updated policy.

19.3 Archival of Previous Versions

Previous versions of this policy are maintained and available for reference. Archived versions document the history of privacy policy changes.

20. Reference Documents

- RBI Guidelines on Digital Lending (2022, updated 2025)
- RBI Outsourcing Guidelines
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
- Digital Personal Data Protection Act, 2023
- Aadhaar Act, 2016
- ISO 27001:2022 - Information Security Management
- RBI Credit Information Policy
- PCI-DSS - Payment Card Industry Data Security Standard (if applicable)
- TCPL Information Security Management System (ISMS) Documentation

21. Enforcement

Compliance & Consequences:

All employees, contractors, vendors, and third parties shall follow this privacy policy in all data handling activities. Non-compliance with any provision of this policy is a serious breach. Violations may result in:

- For Employees: Disciplinary action up to and including termination of employment
- For Contractors/Vendors: Termination of contract and legal action for damages
- For Third Parties: Legal action and regulatory reporting
- For TCPL: Regulatory penalties, fines, and reputational damage

Incident Escalation:

- Any suspected breach or non-compliance must be reported immediately to the CISO
- Failure to report known violations may result in disciplinary action for employees
- Incidents are logged, investigated, and escalated to appropriate authorities if required

Regulatory Reporting:

- Data breaches involving personal information will be reported to the Data Protection Board within mandated timeframes
- Serious regulatory violations will be reported to RBI or other authorities as required by law
- Compliance certifications will be provided to auditors and regulatory bodies

22. Policy Document Management

Document Information:

- Policy Owner: Chief Information Security Officer (CISO)
- Last Updated: November 7, 2025
- Next Review Date: November 7, 2026
- Classification: Internal and Protected

Version Control:

Version	Date	Changes & Reason for Revision
1.0	13-02-2024	Initial issue for ISO 27001:2022 compliance
2.0	07-11-2025	Comprehensive update to include: (a) Digital Lending Guidelines Compliance (Paragraphs 10 & 12), (b) Click-wrap SPDI Rules compliance (Rule 5(1)), (c) Cross-border data transfer controls (Section 16 DPDP Act), (d) Sector-specific RBI and credit bureau regulations, (e) Regulatory watch and contingency planning mechanisms, (f) Staff awareness and training requirements