Sensitive Personal Data or Information (SPDI) and Personal Information Policy

Documented Information Name: Policy Documented Information –SDPI and personal information Policy

Version No: 1.1

Last Updated: 12th September, 2024 Documented Information

Owner- IT Team Reput

Approved By- CTO Reput

Documented Information Management Information

Documented Information Title: Policy Documented Information – SDPI and personal information Policy

Abstract: This documented information is a policy documented information highlighting the policies for Sensitive Personal Data or Information (SPDI) and Personal Information management.

Documented Information Publication History

(All revisions made to this documented information must be listed in chronological order, with the most recent revision at the top)

Type of Information	Documented Information Data
Documented Information Title	Policy Documented Information – SDPI and personal information Policy
Documented Information Code	REPUTIT/ SDPI and personal information Policy
Date of Release	12.09.2024
Documented Information Revision	12-September-2024
Documented Information Owner	IT Department
Documented Information Author(s)	Amit Bishnoi
Checked By	Rohit Mahatma
Security Classification	Internal Use
Documented Information Status	Final

Documented Information Approver List

S. No	Approver	Approver Contact	Signature
1.	Rohit Mahatma- CTO	Rohit@reput.ai	

Documented Information Contact Point

S. No	Documented Information Author	Email
1.	Amit Bishnoi	Amit@Reput.ai

1. Purpose

The purpose of this policy is to establish comprehensive guidelines for the collection, processing, usage, disclosure, and transfer of Sensitive Personal Data or Information (SPDI), Personal Information, and Supply Chain Transaction Data. This policy ensures compliance with applicable global and local data protection laws, such as the General Data Protection Regulation (GDPR), and other relevant regulations. The goal is to protect the privacy of data subjects, including employees, customers, suppliers, and other third parties, while managing supply chain data securely and transparently.

2. Scope

2.1 Applicability:

This policy applies to all employees, contractors, vendors, interns, consultants, and third-party service providers who handle SPDI, Personal Information, or Supply Chain Transaction Data on behalf of Upcycle Reput Tech Private Limited mentioned as "Reput" going forward in document.

2.2 Data Types Covered:

- **Personal Information (PI):** Data that can identify an individual, such as names, contact details, and identification numbers.
- **Sensitive Personal Data or Information (SPDI):** Data requiring extra protection, such as passwords, financial information, health records, and biometric data.
- **Supply Chain Transaction Data:** Information collected from supply chain activities, including but not limited to:
    - Product origin, location, and movement
    - Supplier and manufacturer details
    - Shipment and delivery information
    - Certification and compliance data
    - Transaction timestamps and chain-of-custody records

2.3 Geographical Scope:

The policy applies globally to all locations and environments where Reput operates, including offices, warehouses, data centers, and remote workspaces.

2.4 Data Formats:

The policy governs both digital and physical formats of data.

3. Definitions

3.1 Personal Information (PI):

Data that identifies an individual, such as names, addresses, phone numbers, and email addresses.

3.2 Sensitive Personal Data or Information (SPDI):

Includes information such as passwords, financial details, health and medical information, biometric data, and sexual orientation.

3.3 Supply Chain Transaction Data:
Data collected from the supply chain for traceability purposes, including:

- **Product Origin Information:** Details about where raw materials were sourced or manufactured.
- **Transaction Records:** Data documenting the transfer or movement of goods through the supply chain, including timestamps and locations.
- **Supplier Details:** Information about suppliers, such as company name, address, compliance status, and certifications.
- **Shipping Information:** Data related to the shipment and delivery of goods, including routes, delivery confirmation, and handling instructions.
- **Compliance and Certification Data:** Documentation of regulatory compliance, safety certifications, and quality assurance.

3.4 Data Subject:
The individual or entity to whom personal information or transaction data pertains, such as employees, customers, suppliers, or third parties.

3.5 Data Controller:
Reput, which determines the purpose and means of processing SPDI, Personal Information, and Supply Chain Transaction Data.

3.6 Data Processor:
Any third-party entity that processes data on behalf of Reput.

4. Principles of Data Processing

4.1 Lawfulness, Fairness, and Transparency:

- All data, including supply chain transaction data, must be processed lawfully, fairly, and transparently.
- Data subjects and entities must be informed of how their data will be collected, used, and stored.

4.2 Purpose Limitation:

- Data must only be collected for specific, legitimate purposes. Supply Chain Transaction Data must be collected for traceability, compliance, and efficiency purposes.
- Any further use of data beyond the original purpose requires additional consent or legal justification.

4.3 Data Minimization:

- Only the minimum amount of personal information or supply chain transaction data necessary should be collected.
- Regular assessments must be conducted to ensure data collection practices remain relevant and non-excessive.

4.4 Accuracy:

- Data must be accurate and up to date. Procedures must be established to correct or update data as needed.
- Supply chain data must be verified regularly to ensure the accuracy and reliability of traceability records.

4.5 Storage Limitation:

- Data must not be retained longer than necessary. A data retention schedule for each type of data, including supply chain transaction records, must be maintained.
- Archival and deletion procedures must be secure and compliant with regulations.

4.6 Integrity and Confidentiality (Data Security):

- Security measures must be implemented to protect data from unauthorized access, modification, or loss.
- Supply Chain Transaction Data must be safeguarded to prevent tampering or unauthorized disclosure.

5. Collection of Personal Information, SPDI, and Supply Chain Transaction Data

5.1 Collection Methods:

- **Personal Information and SPDI:** Collected directly from data subjects through forms, applications, or authorized third-party sources. Examples include employment records, financial information for payroll, and health information for insurance purposes.
- **Supply Chain Transaction Data:** Collected through IoT devices, tracking systems, blockchain technology, or manual data entry. This includes data captured at checkpoints, warehouses, and during product transfer between entities.

5.2 Privacy Notices and Consent:

- Data subjects and supply chain partners must be informed about the purpose of data collection and how their data will be used.
- **Consent Management:** Explicit consent must be obtained for processing SPDI. Implied consent may suffice for supply chain data if communicated transparently.

5.3 Legal Basis for Data Collection:
Data collection and processing must be justified by:

- **Consent:** For SPDI and sensitive supply chain data.
- **Contractual Necessity:** To fulfill contractual obligations with supply chain partners.
- **Legal Obligation:** Compliance with regulations, such as product safety laws or financial reporting requirements.
- **Legitimate Interests:** Data collected for legitimate business purposes, such as improving supply chain efficiency.

6. Use of Personal Information, SPDI, and Supply Chain Transaction Data

6.1 Approved Use Cases:

- **Personal Information:** Used for HR management, customer support, and service delivery.
- **SPDI:** Used for payroll, benefits administration, and ensuring workplace safety.
- **Supply Chain Transaction Data:** Used for tracking product movement, verifying origin, compliance reporting, and ensuring supply chain transparency.

6.2 Restrictions on Use:

- Data must not be used for unauthorized purposes, such as marketing or profiling, without consent.
- Automated decision-making using data must be transparent, with human oversight available upon request.

6.3 Anonymization and Aggregation:

- Where possible, personal information and SPDI should be anonymized before use in analytics.
- Supply chain data may be aggregated to provide insights while protecting the privacy of individual entities.
- Data anonymization and pseudonymization processes should follow industry best practices to ensure irreversible de-identification of personal information, especially for SPDI. Anonymized data must meet regulatory standards for data protection and shall be tested periodically to confirm the robustness of anonymization methods.

7. Disclosure and Transfer of Personal Information, SPDI, and Supply Chain Transaction Data

7.1 Internal Sharing:

- Data may be shared internally only with authorized departments or individuals who require it for legitimate purposes.
- Supply Chain Transaction Data must be shared with authorized teams for analysis, reporting, and supply chain management.

7.2 External Sharing and Third Parties:

- **Service Providers:** Data may be shared with third-party vendors for processing, provided they have signed a Data Processing Agreement (DPA) and demonstrated data protection measures.
- **Supply Chain Partners:** Supply chain data may be shared with partners for coordination and compliance purposes. The purpose of sharing must be clearly documented.
- **Regulatory Authorities:** Data must be shared with authorities as required by law, such as during audits or inspections.
- **Regular Audit:** Third-party service providers shall undergo regular compliance audits and assessments to verify their adherence to Reput's data protection standards. Each third party must provide evidence of compliance, such as certifications or audit reports, and agree to maintain the same level of data security and privacy protections as required by this policy.

7.3 Cross-Border Transfers:

- Cross-border data transfers must adhere to international data protection laws. Supply Chain Transaction Data transferred internationally must be protected using safeguards like encryption or contractual clauses.

8. Security Measures

8.1 Physical Security:

- Secure access to physical storage areas where sensitive documents and records are stored.
- Security protocols must be implemented for warehouses and data centers managing supply chain data.

8.2 Technical Security Controls:

- **Encryption:** Personal data, SPDI, and supply chain transaction data must be encrypted at rest and in transit.
- **Access Control:** Role-based access control (RBAC) must be implemented to limit access to data.
- **Network Security:** Firewalls, intrusion detection systems, and anti-malware software must be used to protect digital assets.

8.3 Data Integrity:

- Supply Chain Transaction Data must be protected from tampering using blockchain or digital signatures.
- Integrity checks must be conducted regularly to ensure the accuracy of transaction records.

8.4 Incident Management:

- A protocol for detecting, responding to, and recovering from data breaches or supply chain data tampering incidents must be established.
- All incidents must be documented, investigated, and reported as necessary.

9. Data Retention and Disposal

9.1 Data Retention Schedule:

- **Personal Information and SPDI:** Must be retained for as long as necessary to fulfill its purpose or as required by law.
- **Supply Chain Transaction Data:** Must be retained for a period that supports business needs, legal requirements, or audit purposes.

9.2 Secure Disposal:

- **Digital Data:** Must be erased using certified data destruction methods.
- **Physical Data:** Must be shredded, incinerated, or securely disposed of to prevent unauthorized access.

10. Rights of Data Subjects and Supply Chain Partners

10.1 Right to Access:

- Data subjects can request access to their personal information or SPDI.
- Supply chain partners can request access to their transaction data for verification purposes.

10.2 Right to Rectification:

- Individuals and partners can request corrections to inaccurate data. Requests must be addressed promptly.

10.3 Right to Erasure:

- Data subjects can request the deletion of their personal data if it is no longer needed.
- Supply chain data can only be deleted if it does not violate traceability requirements.

10.4 Right to Restriction of Processing:

- Data subjects can request the restriction of their data processing under certain conditions.

10.5 Right to Object:

- Data subjects have the right to object to data processing that affects their rights or privacy.

11. Employee and Contractor Responsibilities

11.1 Confidentiality Agreements:

- Employees must sign confidentiality agreements and undergo data privacy training.
- Contractors must agree to terms that ensure data protection.

11.2 Data Handling:

- Employees must use secure methods to handle data, such as encrypted communications.
- Supply Chain Transaction Data must be handled with integrity, ensuring accuracy and protection from tampering.

11.3 Reporting Incidents:

- Any suspected data breaches or unauthorized access to supply chain data must be reported to the Data Protection Officer immediately.
- In addition to reporting incidents, periodic compliance audits will be conducted to monitor employee and contractor adherence to data handling, secure disposal, and role-based access protocols. Non-compliance identified during audits will require corrective action to align with Reput's data protection standards.

12. Governance and Accountability

12.1 Data Protection Officer (DPO):

- The DPO oversees compliance, conducts Data Protection Impact Assessments (DPIAs), and manages incidents.

The Data Protection Officer (DPO) shall conduct Data Protection Impact Assessments (DPIAs) for any new projects or processing activities that involve significant volumes of SPDI or that introduce new third-party data sharing. DPIAs are required to evaluate and address potential data privacy risks in advance.

12.2 Supply Chain Integrity Officer (SCIO):

- Responsible for ensuring the integrity of supply chain transaction data and compliance with traceability standards.

12.3 Audits and Reviews:

- Periodic audits must be conducted to ensure compliance with data protection and supply chain standards.

13. Incident Response Plan

13.1 Incident Detection and Reporting:

- Procedures for detecting and reporting data breaches must be established.
- Supply chain data tampering incidents must be escalated immediately to the SCIO and DPO at the email ID- team@reput.ai.
- Regular incident response drills or simulations will be conducted to evaluate the readiness of teams and the effectiveness of response protocols. These drills shall include key response roles and will be evaluated against predefined metrics. Testing will occur at least annually or in response to major policy updates.

13.2 Containment and Investigation:

- Affected systems must be secured, and the scope of the incident determined.
- Incident reports must be prepared and shared with stakeholders as needed.

14. Policy Review and Updates

14.1 Review Schedule:

- This policy will be reviewed annually or as needed based on legal or operational changes.

14.2 Amendments:

- Any updates must be approved by the Data Protection Committee and communicated to all relevant stakeholders.

15. Acknowledgment and Agreement

I acknowledge that I have read, understood, and agree to comply with the SPDI, Personal Information, and Supply Chain Transaction Data Policy of Reput.

Employee/Third party Signature: _____
Employee/Third Name (Printed): _____
Date: _____