Data Privacy Policy

Document control

DOCUMENT NAME	Data Privacy Policy
CLASSIFICATION	Internal
VERSION NUMBER	1.0
DOCUMENT REFERENCE NUMBER	SFL/ISMS/Infosec/Pol-24
DATE	20-10-2023
REVIEWED BY	Ashok Rawat
APPROVED BY	Board of Directors

Revision History

Date	Version	Description	Created by
20-10-2023	1.0	As per RBI Master Direction	Roshani Singh

Documentation status

This is a controlled document. This document may be printed; however, any printed copies of the document are not controlled. The electronic version maintained in the file server and Commune are the controlled copy

Related documents

S.NO.	Document Reference No.	Document Name	Version
1.	SFL/ISMS/Infosec/Pol-01	Policies for Information Security	2.0

Table of Contents

1. Introduction

Confidentiality, Integrity and Availability (CIA) of sensitive data including personal information, regardless of its form and format, must be protected throughout its life cycle against key threats such as unauthorized access/modification and loss of information.

2. Purpose

The purpose of this policy is to outline the SFL's commitment towards meeting its responsibilities to maintain the privacy of personal information. The Data privacy Policy of SFL should outline the types of personal data they collect, how they use and protect that data, and the choices users have regarding their information

3. Scope

This policy is applying to:

- Information Assets that store the Hard copy/Electronic information
- All employees of SFL
- All third-party employees who work on SFL's premises or connect remotely from their networks to SFL's network.
- Customer personal data refers to the specific types of information that SFL collects, uses, and stores about its customers, such as names, addresses, email, Mobile numbers, Preferences, interests, Adhaar card pan card and references.

4. Terms and definitions

i. **Database Owner-** is a specialized computer systems administrator who maintains a successful database environment by directing or performing all related activities to keep the data secure. The top responsibility of a DBA professional is to maintain data integrity.

ii. **Data Custodian-** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purposes for and how personal data is processed or is to be processed.

iii. **Data Portability-** means the ability for data to be transferred easily from one IT system or computer to another through a safe and secure means in a standard format.

iv. **Consent of the data subject**- means any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

v. **Data facts and statistics-** collected for reference or analysis.

vi. **Database-** is a structured set of data held in a computer, especially one that is accessible in various ways.

vii. **Data Subject/PII Principal** - means an identifiable person; one who can be identified directly or indirectly, in particular by reference to an identification number or one or more factors specific to his physical, physiological, economic, cultural, or social identity

viii. **Personal Data** - any information that relates to an identified or identifiable living individual. Different pieces of information, which when collected can lead to the identification of a particular person, also constitute personal data.

ix. **Data breach** - A data breach is a security incident in which information is accessed without authorization

x. **Record-** means public records and reports in credible news media

xi. **Sensitive Personal Data** - means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trades union membership, criminal records, or any other sensitive personal information

5. Policy statements

- SFL shall ensure privacy of personal information including sensitive personal information of its customers, employees, vendor employees & contracted employees/consultants /auditors.
- Personal information shall constitute the following:
    - Name, Age.
    - Contact information including email address
    - Demographic information such as postcode, email IDs, Mobile numbers, Preferences, and interests.
- SFL should establish the necessary technical and security measures to prevent unauthorized or unlawful access to, accidental loss of, destruction, or damage to Information. To ensure the safety of Information of SFL, secured web services should be configured to run within a virtual private connection and an SSL certificate to make sure that all communications are made over HTTPS, and SFTP using TLS. The strategies SFL shall use to guarantee data privacy internally include secure data storage, the use of data encryption technologies, the creation of organizational policy for handling personal data and other sensitive or confidential data, and ongoing capacity building for all staff.

6. Responsibilities

Roles	Responsibilities
Business Head/Department Heads	• Responsible for adherence and implementation of Data Privacy Policy. • Responsible for updating Critical Data register if any critical data is added, changed or removed. • Information Security team.
Data Owners	• Classifying and labeling information with the appropriate classification level. • Periodically reviewing the classification level of information and reclassifying them when appropriate. • Understand the uses and risks associated with the information for which they are accountable. This means that they are responsible in case of any improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security-related control deficiencies pertaining to the information for which they are the designated Owner. • Responsible for choosing appropriate information systems, and relevant controls for information handled by these systems, consistent with policies and standards issued by the IT Department.
Data Custodian	• Individuals/staff members, in physical or logical possession of information from Owners. • Primary responsibility is to maintain the Confidentiality, Integrity and Availability of data. • Highlight any unaddressed risk to the Information owner.

7. Procedures

7.1. Data privacy

Information Security team should conform to the following principles for Personal Information Collection:

- **Collection Limitation**: Personal information should be collected for specified and legitimate purposes only. The information SFL collects shall be used to provide the Service to the customer, to improve the quality of the Website and Service, and to communicate information about the Service. SFL shall never sell Client information or trade or share with other companies or organizations for

commercial purposes or otherwise, unless they have been expressly authorized by the customer, either in writing or in electronic form. The customer's Personal Information should be collected primarily from the customer. However, SFL may also obtain information about customers from other sources in order to verify the information submitted by customers.

- **Purposes Specification:** The purposes, for which Personal information is collected, should be based on the approved business requirement. The purpose should be identified & specified at or before the time the information is collected. SFL shall use the collected information to provide, improve, customize, support, and market its services.

    - SFL services operates and provides services including customer support improving, and customizing services. SFL understands how customers use their services and analyze the information to evaluate and improve services, develop and test new services and features, and conduct troubleshooting activities.
    - SFL communicates with clients about SFL's services and features. They should also inform clients about SFL's terms and policies from time to time.

- **Personal information Quality:** Personal information should be relevant to and not excessive for the purposes for which it is collected and used. Personal information should be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
- **Lawful Processing of customer data:** Personal data of customers will be securely stored, in manual or electronic form, and in accordance with the IT Act, 2022. In addition, data collected for a specific purpose, product, or service may be stored in SFL with other information relating to an individual, and only in accordance with the data privacy principles mentioned above.
- The Data Fiduciary will be responsible for processing the data.

- **SFL shall process information in the following cases-**

    - When the data subject has given consent to process his or her data for one or more specific purposes.
    - When Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject before entering into a contract.
    - Processing is necessary for compliance with a legal obligation to which SFL is subject.
    - Processing is necessary to protect the vital interests of the data subject or another person.
    - The Data Custodian can process the personal data in case of a medical emergency involving a threat to life or immediate threat to the health of the Data Subject or any other individual.

- A Data Subject has the right to complete, correct, update, and delete their personal data.
- A Data Subject has the right to nominate, in the event of death or incapacity of the Data Subject, exercise the rights of the Data Subject.

- **Consent:** The knowledge and consent of the individual should be ensured for the collection/ receiving, usage, storage, or disclosure of personal information. SFL's business operations shall be guided by the following:
  - The company shall request for consent in a manner, which is distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language, where the data subject's consent should be given in the context of a written declaration.
  - SFL shall inform the data subject of his/her right and the ease to withdraw his/her consent at any time.
  - To ensure effective identification, email addresses and passwords should be used.
  - Device IDs should be used to ensure that the right devices are being managed.
  - SFL shall request the consent of the data subject where the data may be transferred to a third party for any reason.
  - SFL shall only obtain personal information for the specific purpose of collection after which consent should be taken from the data subject to process his or her data.
  - If the Data Subject's data is being used without their consent or in a wrongful manner then they're eligible to file a complaint.
  - The consent Manager shall be accountable to the Data Subject and shall act on their behalf.

- **Limitation on Use and Retention:** Personal information should not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information should be kept only as long as it is necessary for the purposes for which it was collected and processed and in accordance with Personal information storage requirements under applicable IT Act, 2022. The retention period of different types of data shall be defined and maintained based on the respective approved business requirements. Legal Dept. will advise the respective Business Head/Department Head for enforcement of the retention period of Personal Information.

- **Disclosure of Personal Information:** The information Security Team should not disclose, sell, or otherwise distribute to any third party any Personal information without prior consent of individual except under the following circumstances:

  - **Compliance with legal obligations**: SFL may also disclose your personal information as required by law when it is considered in good faith that

disclosure is necessary to protect the company's safety or the safety of others, to investigate fraud, or to respond to a government request. Where possible and legally permissible, SFL shall communicate with the client in advance of any such disclosure. SFL shall reject any third-party requests for personal information that are not legally binding.

- **Third-party service providers –** SFL may, from time to time, outsource some or all the operations of our business to third-party service providers. In such cases, it shall be necessary for SFL to disclose personal information to those service providers. In some cases, the service providers may collect Personal Information directly from the individual(s) on SFL's behalf. These service providers may have access to individuals' Personal information needed to perform their functions. However, SFL shall ensure secure processes are followed by such service providers to access, use, and disclose personal information.

As permitted or required by any law/statute/regulator, the personal information provided to the third-party service providers is disclosed:

- To protect or defend SFL's rights, interests, and property or the same of our associates and affiliates, or our affiliate's employees, consultants, etc.
- For fraud-prevention purposes
- To prevent any persons, including insurers and lenders who supply benefits or services to the individual

- **Reasonable Security practices:** All appropriate technical, physical, and organizational measures should be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to data. SFL follows the best security practices in line with ISO 27001 standards, to help in preventing unauthorized access to any customer's information.

- **Procedures and Guidelines for Data Privacy:** SFL maintains physical, technological and procedural safeguards and security that comply with the IT Act, 2022. In addition, training procedures are in place for all employees of SFL to ensure high standards in relation to Data Privacy. Below are some of the steps that SFL has taken to ensure customer data privacy
  - The entire customer's data is classified as per SFL data classification guidelines.
  - Access to sensitive data should be provided strictly on the basis of need to know.
  - Backup on a removable storage media should be kept in a safe and secure environment.

8. Data Deletion

Data Deletion outlines the guidelines for the secure and systematic removal of data from SFL's systems to ensure compliance with data protection regulations, safeguard privacy, and reduce the risk of unauthorized access to obsolete or unnecessary information.

- SFL shall classify data based on sensitivity and relevance to determine the appropriate deletion procedures.
- SFL shall adhere to applicable data protection laws and regulations, ensuring the right to be forgotten and compliance with privacy requirements.
- SFL shall designate data owners for each dataset who are responsible for determining the appropriate retention period and overseeing the deletion process.
- SFL shall utilize secure methods for data deletion, including permanent erasure techniques that prevent data recovery.
- SFL shall establish specific timelines for data deletion based on regulatory requirements and business needs. Regularly review and update these timelines.
- SFL shall communicate data deletion policies and procedures to relevant stakeholders, ensuring awareness and cooperation across the organization.

9. Data Masking

In adherence to SFL's commitment to data privacy and confidentiality, it also includes provisions for the secure and responsible use of data masking techniques to safeguard sensitive information during non-production activities. The primary objective is to ensure the protection of privacy and compliance with data protection regulations.

- SFL shall clearly identify and classify sensitive data elements that require masking, such as personally identifiable information (PII), financial data, and other confidential information.
- SFL shall extend data masking practices consistently across different environments, including development, testing, and staging, to maintain data integrity and privacy in various scenarios.
- SFL shall implement appropriate data masking methods, such as substitution, shuffling, encryption, or tokenization, based on the sensitivity of the data and specific use cases.
- SFL shall enforce access controls to restrict access to unmasked data, and implement robust logging mechanisms to capture details of data masking activities, supporting accountability and auditability.

10. Transfer of Information

SFL or any person on our behalf may transfer your Information including Personal Information /Sensitive Personal Data or Information, to any other body corporate or a person in India, or

located in any other country, that ensures the same level of Data protection that is adhered to by Us if such transfer is necessary for the performance of the lawful contract between Us or any person on our behalf and you, or where you have consented to such transfer.

11. Correction of Discrepancies

SFL or any person on its behalf shall permit you as and when requested by you to review the Information you had provided and ensure that any Personal Information or Sensitive Personal Data or Information found to be inaccurate or deficient shall be corrected or amended as feasible provided that SFL shall not be responsible for the authenticity of the Personal Information or Sensitive Personal Data or Information supplied by the you to SFL or any person acting on its behalf.

12. Option to withdraw Consent

SFL or any person on its behalf shall, prior to the collection of Information including Sensitive Personal Data or Information, provide you an option to not to provide the data or Information sought to be collected. You shall, at any time while availing the services or otherwise, also have an option to withdraw your consent given earlier to SFL. Such withdrawal of the consent shall be sent in writing to SFL. In the case that you do not provide Information including Sensitive Personal Data or Information, or later on withdraw your consent, SFL shall have the option not to provide you the services for which the said Information including Sensitive Personal Data or Information was sought.

13. Redressal of Grievances

SFL shall address any grievances that you may have with respect to processing of Information including Sensitive Personal Data or Information, in a time bound manner. For this purpose, SFL designates **Mr. Vikas Umrao** as the Grievance Officer and the contact detail of the Grievance Officer is clientgrievance@SFLcreditcare.com The Grievance Officer shall redress the grievances expeditiously but within one month's time from the date of receipt of grievance. If you have any questions or concerns about our use of your Personal Information including Sensitive Personal Data or Information, please contact the Grievance Officer using the contact details provided in this Policy.

14. Updates to privacy policy

SFL shall update this Privacy Policy from time to time to reflect changes in their practices or legal requirements. Updated versions shall be posted on the company's website, and users should be encouraged to review the policy periodically.

15. Policy exceptions & retention

A policy exception represents a circumstance whereby an employee of SFL knowingly deviates from a requirement of the Policy. All Policy exceptions must be approved by the senior management.

All such documentation shall be maintained in accordance with the SFL policy for the Retention of Documents and Records.