Data Privacy Policy

History of Revisions

Version	Summary of Revisions	Date of Approval
2.0	Annual Review	23-12-2022
1.0	Policy Formulation	23-09-2021

Table of Contents

1. Preamble

Equitas Small Finance Bank (ESFB) is committed to protecting its customer privacy. ESFB conducts its business in compliance with the applicable laws on data privacy protection and data security in India. This privacy policy broadly deals with the protection of personal information that ESFB collects from its customers / clients during the course of their dealings with ESFB.

1.1 Objective of the Policy

The objective of this Policy is to provide a framework for ESFB for collection, usage, disclosure, storage, disposal of customer information acquired during the course of its business. The Policy also stipulates the responsibilities of the persons whose data is in the possession of ESFB.

1.2 Scope of the Policy

This policy is applicable to all employees of ESFB and third parties including customers, business partners and any individual availing the services and / or products of ESFB. This policy is also applicable to all persons who collect, store, process the data of individuals on behalf of ESFB

This Policy is applicable in respect of personal information and sensitive personal data/information collected by the Bank/Bank's associates directly from the customer or through the Bank's online portals, mobile apps and electronic interactions.

1.3 Definitions

Personal data: Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

Password: "Password" means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information.

2. Regulatory Framework Applicable Regulations

2.1 The Information Security Act, 2000

2.1.1 Compensation for failure to protect data: Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. (Section 43A)

2.2 Ministry of Communications and Information Technology (Department of Information Technology) Notification, New Delhi, dated 11th April, 2011.

2.2.1 Sensitive Personal Data (Rule 3) - Sensitive personal data or information of a person means such personal information which consists of information relating to:

(i) password;
(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
(iii) physical, physiological and mental health condition;
(iv) sexual orientation;
(v) medical records and history;
(vi) Biometric information;
(vii) any detail relating to the above clauses as provided to body corporate for providing service; and
(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise

Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of this policy.

2.2.2 Body corporate to provide policy for privacy and disclosure of information (Rule 4) - The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

(i) Clear and easily accessible statements of its practices and policies;
(ii) type of personal or sensitive personal data or information collected under rule 3;
(iii) purpose of collection and usage of such information;
(iv) disclosure of information including sensitive personal data or information as provided in rule 6;
(v) Reasonable security practices and procedures as provided under rule 8.

2.2.3 Collection of information (Rule 5) –

(1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless — (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of — (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they 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 a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such body corporate or any other person acting on behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

2.2.4 Disclosure of information. (Rule 6) –

(1) Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation: Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

(2) Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

(3) The body corporate or any person on its behalf shall not publish the sensitive personal data or information.

(4) The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

2.2.5 Transfer of information (Rule 7) - A body corporate or any person on its behalf may transfer sensitive personal data or information including any 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 the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

2.2.6 Reasonable Security Practices and Procedures (Rule 8) –

(1) Body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security

programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

3. ESFB Policy framework

3.1 Policy Guidelines

ESFB will follow the definition of sensitive personal data/information of a person as per paragraph 2.2.1 of this Policy.

3.2 Collection of Information

Type of information collected by the Bank:

- For products and services, ESFB may/will collect information, as applicable, such as name, date of birth, address, age, income and assets and liabilities of individuals/organization/ company/ firm /any entity along with other relevant financial and project and proposal details.

- Financial information, including but not limited to, account balances, payment history; account usage, etc., of individual /organization/ company / firm / any entity is also called for from the customers' bankers for validation.

  Any other information necessary for providing the products/services sought by the customer/client as well as information required to be obtained as per regulations/statutes.

3.3 Mode of collection of information:

- ESFB may also collect information on the agreements that the customer may have signed with third party/government agency.

- ESFB may collect the data of individuals, wherever video surveillance is in place, which are personally identifiable in nature.

- ESFB may collect, through their application opening forms or any such instrument, websites and mobile applications provided by ESFB personal information (such as name, date of birth, business dates, job title, company, address, telephone number and personal and official e-mail addresses), which the customer may knowingly provide (e.g. for sending any queries through our website, mobile applications.), for use in our commercial relationship.

- Any other mode of collection of information with the consent of the provider of the information.

- Collection of the information/data shall be based on the consent of the individual / individual representing firm.

3.3.1 Purpose of Data Collection:

- To provide customers with customized options in dealing with their financial services / products and credit proposals depending on the information provided by them.

- To ensure that ESFB has all the relevant information to assess the financial and project proposal submitted by the customers.

- The information shall be used for such purposes connected with the functions or activities of ESFB or any person on its behalf.

- To meet the legal and regulatory requirements.

3.3.2 The Bank or persons/entities authorized by the Bank shall obtain consent in writing through letter or Fax or email or through any other electronic/paper form, from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

3.3.3 Bank or persons/entities authorized by the Bank shall not collect sensitive personal data or information unless — (a) the information is collected for a lawful purpose connected with a function or activity of the Bank or any person on its behalf; and (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

3.3.4 While collecting information directly from the person concerned, the Bank or any person/entity on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of — (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — (i) the agency that is collecting the information; and (ii) the agency that will retain the information.

3.3.5 Bank or any person/entity on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. The Bank shall retain the data only in accordance with the terms agreed with the data provider at the time of obtaining the same and as per regulatory guidelines.

3.3.6 The Bank shall use the information collected for the purpose for which it has been collected.

3.3.7 Bank or any person/entity on its behalf permit the providers of information, as and when requested by them, to review the information they 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.

3.3.8 Bank shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information.

3.3.9 Bank or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the Bank. Such withdrawal of the consent shall be sent in writing to the Bank. In the case of provider of information not providing or later on withdrawing his consent, the Bank shall have the option not to provide goods or services for which the said information was sought.

3.4 Disclosure of Information

3.4.1 Disclosure of sensitive personal data or information by the Bank to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the Bank and provider of information, or where the disclosure is necessary for compliance of a legal obligation. The sharing/disclosure of data shall only be in accordance with the terms agreed with the data provider at the time of obtaining the same

3.4.2 Information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences; provided the request from Government agency is received in writing.

3.4.3 Any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.

3.4.4 The Bank or any person on its behalf shall not publish the sensitive personal data or information.

3.5 Transfer of information:

The Bank or any person on its behalf may transfer sensitive personal data or information including any 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 the Bank. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the Bank or any person on its behalf and provider of information or where such person has consented to data transfer.

3.6 Reasonable Security Practices and Procedures:

Bank or a person on its behalf shall implement such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the Bank or a person on its behalf shall demonstrate, as and when called upon to do so by the agency mandated under

the law, that the Bank or a person on its behalf has implemented security control measures as per their documented information security programme and information security policies.

Access to customer account(s) information is given to only those employees involved in providing the services to the customers on a 'need to know' basis. All ESFB employees are required to keep all customers' information confidential in accordance with the terms of the employment.

3.7 Non-Personal Data Collected Automatically:

When the customer accesses ESFB Website or mobile banking applications, ESFB may automatically (i.e., not by registration) collect non-personal data (e.g. type of Internet browser and operating system used, domain name of the website from which the customer visited the website, number of visits, average time spent on the site, pages viewed, etc.). ESFB may use this data and share it with its affiliates to monitor the utility and attractiveness of its websites and improve their performance or content.

3.8 'Cookies' – Information stored automatically on your computer:

When customer views ESFB Website, ESFB may store some data on customer's computer in the form of a "cookie" to automatically recognize the computer the next time the customer visits the ESFB website. Cookies can help ESFB in many ways, for example, by allowing ESFB to tailor a Website to better match customer interests or to store passwords to save customer the trouble of having to re-enter it each time. If the customer does not wish to receive cookies, the customer may configure his/her Internet browser to erase all cookies from his/her computer's hard drive, block all cookies or to receive a warning before a cookie is stored.

3.9 Obligation of Provider of Information:

By using the Bank's account opening application forms or any such instrument for collecting data from the provider of the information or providing information through website or mobile applications provided by ESFB or providing information by any other means, the provider of the information acknowledges that he/she in his/her individual capacity or representing any entity / organization /firm /company understands and agrees to be bound by this Privacy Policy.

3.10 Jurisdiction and Applicable Law:

This Data Privacy Policy shall be governed by the laws of India and shall be subject to the exclusive jurisdiction of the courts located in Chennai.

3.11 Display on website

A copy of the Board approved privacy policy will be displayed on the website of the Bank as per regulations, for ease of reference of its customers/vendors/third parties/business partners and any individual availing the services and / or products of ESFB.

3.12 Changes to this Policy:

ESFB reserves the right to modify this Data Privacy Policy from time to time, without any notice, in order to ensure that it accurately reflects the regulatory/statutory environment and our data collection needs. When material changes are made to this Data Privacy Policy, ESFB will post the revised Policy on its website.

4. Provisions in policy over and above but in consonance with RBI guidelines

None

5. Changes to the Policy

Not Applicable

6. Periodicity of Review of the Policy

The Board will review this policy on need basis and as may be required under the regulations/statutes that may be issued in future.

Author of the Policy	Chief Information Security Officer
Reviewer of the Policy	Chief Compliance Officer
Name of Committee which recommended to the Policy Formulation Committee of the Board	Executive Policy Formulation & Review Committee
Date of Board Approval	23-Dec-2022
Date of Next Review	18-24 months from the date of board approval / previous review