



SHIVA SAHAKARI BANK NIYAMITHA

DAVANGERE-577001

DATA PRIVACY POLICY

Document Control

Document Name	Data Privacy Policy
Classification	Internal and Confidential
Document#	SHIVA SAHAKARI BANK NIYAMITHA DAVANGERE
Version	1.0
Date Released	01-MAY-2025

Document Ownership

Prepared By:	IT Department	Document Owner	IT Department
Approved By:	Board of Directors		

Copyright ©2025 Shiva Sahakari Bank Niyamitha Davangere. All Rights Reserved. This document contains sensitive & confidential information, and should not be disclosed to third parties without the prior written consent of Shiva Sahakari Bank Niyamitha Davangere. No part of this publication is reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Shiva Sahakari Bank Niyamitha Davangere.

Sl No	Descriptions	Page NO
	Privacy Commitment:	3
1	Definitions	3
2	Personal Information	3
3	Scope	4
4	Applicability of the Policy	4
5	Introduction:	4
6	Purpose of Collection and use of personal information / sensitive Personal Data or Information	4
7	Requirement for information collection:	4
8	Consent	5
9	Usage of information	5
10	Information sharing	5
11	Reasonable security practices and Procedures	6
12	Information protection	6
13	Retention and disposal:	6
14	Amendments/Notice of change:	7
15	Cookie Policy:	7
16	DATA PRIVACY OF BENEFICIARY AADHAAR HOLDER	7
	16.1 Introduction:	7
	16.2 Aadhaar Authentication Services:	7
17	Data Privacy on Aadhaar and Biometric details	8

Privacy Commitment:

Shiva Sahakari Bank Niyamitha Davangere recognizes the expectations of its customers with regard to privacy, confidentiality and security of their personal information that resides with the Bank. It is the policy of the Bank to keep the personal information of customers secure and use the same solely for the activities related to the Bank. The Bank has adopted the privacy policy aimed at protecting the personal information provided by/disclosed by the customers. This Policy governs the way in which the Bank collects, uses, discloses, stores, secures and disposes of personal information and sensitive personal data or information.

1. Definitions:

“Personal information” (PI) means any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with the Bank, is capable of identifying such person.

“Sensitive personal data or information” (SPDI) of a person means such personal information, which consists of information relating to:

- Password;
- Financial information such as Bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records & history;
- Biometric information;
- Any detail relating to the above clauses as provided to body corporate for providing service;
- Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract otherwise.

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

2. Personal Information:

Includes but not limited to, financial information including banking and related information, financial and credit information, ethnicity, caste, race or religion, health related details of the individuals, sexual orientation, medical records and history, biometric information, email, address, PAN, TAN, payment card information, photographs; provided that, 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.

Privacy Policy refers to privacy commitment of the Bank services as specified in this document.
third party refers to an entity that is not the bank or its direct customer.

3. Scope:

This policy covers all users who interact with bank and those whose personal information is collected or received or transmitted or processed or stored or dealt with or handled by bank. This policy covers the “sensitive personal data or information” of the persons handled by bank in any form or mode.

Please note that this Privacy Policy does not extend to third party websites linked to bank websites, if any.

Any information that is freely available or accessible in public domain or furnished under any other law for the time being in force shall not be financial and credit information, ethnicity, caste, race or religion, health related details of the individuals, sexual orientation, medical records and history, biometric information, email, address, PAN, TAN, payment card information, photographs; provided that, 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.

4. Applicability of the Policy

This policy is applicable to the personal information and sensitive personal data or information collected by the Bank or its affiliates directly from the customer or through the Bank’s online portals mobile apps and electronic communications as also any information collected by the Bank’s server from the customer’s browser.

5. Introduction:

The Bank is committed to respect the privacy and use of personal information responsibility. The bank is guided by the regulations and best practices in the area of privacy. If customer is providing certain information with which that customer can be identified personally, then customer can be assured that it will only be used in accordance with the privacy policy.

6. Purpose of Collection and use of personal information / sensitive Personal Data or Information:

The Bank collects the PI and SPDI from its customers and uses the same for specific business purposes or for other related purposes designated by the Bank or for a lawful purpose to comply with the applicable laws and regulations. The Bank shall not divulge any personal information collected from the customer, for cross selling or any other purposes, without the written consent of the customer.

The authenticity of the personal information provided by the customer shall not be the responsibility of the Bank.

The Bank shall not be responsible for any information that is freely available or accessible in public domain or furnished as per law for the time being in force.

7. Requirement for information collection:

Bank collects and uses the financial information and other personal information from its customers as is required under various regulations and guidelines including the KYC/E-KYC/C-KYC norms of RBI. Such information is collected and used for specific business purposes or for other related purposes designated by bank or for a lawful purpose to comply

with the applicable laws and regulations.

8. Consent:

By providing the personal information, the persons provide consent to the bank to use personal information for the usage of the information for the product or services requested or applied or shown interest in and/or to enable bank for personal verification and or process applications, requests, transactions and/or maintain records as per internal or legal or regulatory requirements and shall be used to provide the persons with the best possible services or products as also to protect interests of the bank.

9. Usage of information:

Bank may use Personal Information:

To allow customers to apply for products or services and evaluate customer eligibility for such products or services:

- To verify customer identity and/or location in order to allow access to accounts, conduct online transactions and to maintain measures aimed at preventing fraud and protecting the security of account and personal information
- For risk control, for fraud detection and prevention, to comply with laws and regulations and to comply with other legal process and law enforcement requirements;
- To inform customer about important information regarding the site, products or services for which customer apply or may be interested in applying for, or in which customer are already enrolled, changes to terms, conditions, and policies and/or other administrative information;
- For business purposes, including data analysis, audits, developing and improving products and services, enhancing the site, identifying usage trends and determining the effectiveness of promotional campaigns;
- To allow customer to utilize features within our sites by granting bank access to information from customer device such as contact lists, or Geo-location when customer request certain services
- To respond to customer inquiries and fulfill customer requests;
- To deliver marketing communications that we believe may be of interest to customer, including, ads or offers tailored to customer;
- To personalize customer experience on the site;
- To allow customer to use some site financial planning tools, information that customer enter into one of these planning tools may be stored for future access and use. Customer will have the option not to save the information;

Bank will not be held responsible for content, information usage and privacy policies of linked site which will not be under the control of the bank. The authenticity of the personal information provided by the customer will not be the responsibility of bank.

10. Information sharing:

- ❖ The Information shall be shared with any external organization or persons to enable bank to provide services or to enable the completion or compilation of a transaction, credit reporting, or the same is necessary or required pursuant to applicable norms or pursuant to the terms and conditions applicable to such information as agreed to with bank or pursuant

to any requirement of law or regulations or any government or court or other relevant authority's directions or orders.

- ❖ Information may be disclosed without obtaining persons prior consent, with government agencies mandated under the law where disclosure is necessary for compliance to legal obligations. Any information may be required to be disclosed to any third party by bank by an order under the law for the time being in force.
- ❖ It may be necessary to disclose the information to one or more agents and contractors of bank and their sub-contractors, but such agents, contractors, and sub-contractors will be required to agree to use the information obtained from bank only for specific assigned purposes and will be disposing the information in a secured manner consistent with bank's policies.
- ❖ The persons authorizes bank to exchange, share, part with all information related to the details and transaction history of the covered persons to its affiliates or banks or financial institutions or credit bureaus or agencies or participation in any telecommunication or electronic clearing network as maybe required by law, customary practice, credit reporting, statistical analysis and credit scoring, verification or risk management or any of the aforesaid purposes and shall indemnify bank for use or disclosure of this information.

11. Reasonable security practices and Procedures:

The Security of personal information is a priority and is protected by maintaining physical, electronic and procedural safeguards that meet applicable laws. The Bank shall take reasonable steps and measures to protect the security of the customer's personal information from misuse and loss, unauthorized access, modification or disclosure. The Bank maintains its security systems to ensure that the personal information of the customers is appropriately protected. The Bank ensures that its employees and affiliates respect the confidentiality of any personal information held by the Bank.

12. Information protection:

Bank customers have access to a broad range of products and services such as basic Banking Products, ATM, Mobile Banking, AePS, EKYC etc. To deliver products and services effectively and conveniently, it is extremely important that the bank uses technology to manage and maintain certain customer information while ensuring that customer information is kept confidential and protected.

Bank is committed in ensuring that the information is secure. In order to prevent unauthorized access or disclosure, bank has put in place reasonable physical, electronic and managerial procedures to safeguard and secure the information that bank collects.

13. Retention and disposal:

Bank's current policy to retain information for so long as it is needed by the business. Since most information is in continuous use, much is retained on an indefinite basis or for such period to satisfy legal, regulatory or accounting requirements.

When bank finds that information collected or stored or transferred is no more in use and if there is no legal obligation to retain such information, bank will determine appropriate means to dispose or to de-identify personally identifiable information in a secure manner in keeping with its legal obligations.

14. Amendments/Notice of change:

The Bank may, from time to time, change this, Policy. The customers are advised to visit the site and go through the privacy policy as bank modifies the policy from time to time as, bank constantly absorbs advanced technology and redefines processes.

15. Cookie Policy:

The Bank's digital platforms may use various third-party analytical tools. These tools may use cookies which are downloaded to the customer's device when the customer visits a website in order to provide a personalized browsing experience. Cookies are used for other purposes like remembering the customer's preferences and settings, provide personalized browsing experience and analyze site operations. These Cookies collect information about how users use a website. All information collected by these third-party cookies is aggregated and anonymous. By using the Bank's website, the user agrees that these types of cookies can be placed on his/ her device. User is free to disable/ delete these cookies by changing his/ her device / browser settings. The bank is not responsible for cookies placed in the device of user/s by any other website and information collected thereto.

16. DATA PRIVACY OF BENEFICIARY AADHAAR HOLDER

16.1 Introduction:

The Unique Identification Authority of India (UIDAI) has been established by the Government of India with the mandate to the Authority is to issue a unique identification number (called Aadhaar or UID) to Indian residents that is robust enough to eliminate duplicate and fake identities, and can be verified and authenticated using biometrics in an easy and cost-effective manner.

The UID has been envisioned as a means for residents to easily and effectively establish their identity, to any agency, anywhere in the country, without having to repeatedly produce identity documentation to agencies.

The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically through presentation of their fingerprints / iris authentication or non- biometrically using a One Time Password (OTP) sent to the registered mobile phone or e-mail address.

16.2 Aadhaar Authentication Services:

Aadhaar Authentication is defined as the process wherein, Aadhaar number along with the Aadhaar holder's personal identity information is submitted to the Central Identities Data Repository (CIDR) for matching following which the CIDR verifies the correctness thereof on the basis of the match with the Aadhaar holder's identity information available with it.

The purpose of Authentication is to enable Aadhaar-holders to prove identity and for service providers to confirm the resident's identity claim in order to supply services and give access to benefits. To protect resident's privacy, Aadhaar Authentication service responds only with a "Yes/No" and no Personal Identity Information (PII) is returned as part of the response.

16.3 Data Privacy on Aadhaar and Biometric details: -

The submission of Aadhaar details by a customer to the Bank is voluntary, and the Bank will not insist on a customer to produce their Aadhaar details for availing any of the services. In cases where Aadhaar number is offered voluntarily by the customer to the Bank, the Bank will seek a declaration by the customer towards the same.

For cases where e-KYC verification is required, the Bank will get an explicit consent from the resident for download of resident demographic details from UIDAI mentioning the purpose for which the details are sought. The consent will be either in the form of an authorization letter or a provision to electronically record the consent in a software application. Biometric details will also be required to be captured by the Bank for purposes of authentication, for example to authenticate a customer before permitting transaction through a Micro ATM / any other device, as an AEPS (Aadhaar Enabled Payment System) transaction. The biometric details whenever captured by the Bank will be used only for data exchange with UIDAI which validates the captured biometric data against the biometric data maintained in CIDR (Central Identities Data Repository) against the specific Aadhaar number. The Bank will use STQC certified devices for capturing biometric details and secured network for transmission. While the demographic details received from UIDAI will be stored for future reference, the biometric details will not be stored by the Bank in any manner and form. A system log wherever required will be maintained to extract the details in case of disputes. The logs will capture Aadhaar Number, timestamp etc., but will not capture / store the PID (Person Identity Data) associated with the transaction.

The services will be offered at select branches identified by the Bank. Aadhaar enrollment and updation entails the process of capturing the personal information of the customers along with their Biometric details (Finger print and iris biometrics). To protect data privacy, the enrollment application sought by the Bank from the customer to assist in internal data entry process will be returned to the resident / will be destroyed internally. The data so captured will be sent to UIDAI as a straight through process. The Bank will not store the data captured (both biometric and personal information) in any manner and form.

Bank shall not publish any personal identifiable data including Aadhaar in public domain/websites etc.
