

Yadrav Co-Op Bank Ltd; Yadrav

Privacy Policy

1.0 Scope

This policy is applicable to all Bank employees, contractors, vendors, interns, associates, customers and business partners who may receive personal information, have access to personal information collected or processed, or who provide information to the organization. This Policy applies to all Bank employees, contractors, vendors, interns, associates, customers and business partners who receive personal information from Bank, who have access to personal information collected or processed by Bank, or who provide information to Bank, regardless of geographic location. All employees of Bank are expected to support the privacy policy and principles when they collect and / or handle personal information, or are involved in the process of maintaining or disposing of personal information. This policy provides the information to successfully meet the organization's commitment towards data privacy. All partner firms and any Third-Party working with or for Bank, and who have or may have access to personal information, will be expected to have read, understand and comply with this policy. No Third Party may access personal information held by the organization without having first entered into a confidentiality agreement.

2.0 Definition

A privacy policy is a statement or legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data

3.0 Collection of Personal Information

Personal information may be collected online or offline. Regardless of the collection method, the same privacy protection shall apply to all personal information. Personal information shall not be collected unless either of the following is fulfilled: the data subject has provided a valid, informed and free consent; processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract; processing is necessary for compliance with the organization's legal obligation; processing is necessary in order to protect the vital interests of the data subject; or processing is necessary for the performance of a task carried out in the public interest. Data subjects shall not be required to provide more personal information than is necessary for the provision of the product or service that data subject has requested or authorized. If any data not needed for providing a service or product is requested, such fields shall be clearly labeled as optional. Collection of personal information shall be avoided or limited when reasonably possible. Personal information shall be de-identified when the purposes of data collection can be achieved without personally identifiable information, at reasonable cost. When using vendors to collect personal information on the behalf of Bank, it shall ensure that the vendors comply with the privacy requirements of Bank as defined in this Policy.

Bank shall at minimum, annually review and monitor the information collected, the consent obtained and the notice / SoW / contract agreement identifying the purpose. The project team/support function shall obtain approval from the IT Security team before adopting the new methods for collecting personal information electronically. Bank shall review the privacy policies and collection methods of Third-Parties before accepting personal information from Third-Party data sources.

Personal information may only be used for the purposes identified in the notice / SoW / contract agreements and only if the data subject has given consent;

Personal information shall be retained for as long as necessary for business purposes identified in the notice / SoW / contract agreements at the time of collection or subsequently authorized by the data subjects. When the use of personal information is no longer necessary for business purposes, a method shall be in place to ensure that the information is destroyed in a manner sufficient to prevent unauthorized access to that information or is de-identified in a manner sufficient to make the data non-personally identifiable. Bank shall have a documented process to communicate changes in retention periods of personal information required by the business to the data subjects who are authorized to request those changes.

Personal information shall be erased if their storage violates any of the data protection rules or if knowledge of the data is no longer required by Bank or for the benefit of the data subject. Additionally, Bank has the right to retain the personnel information for legal and regulatory purpose and as per applicable data privacy laws. Bank shall perform an internal audit on an annual basis to ensure that personal information collected is used, retained and disposed-off in compliance with the organization's data privacy policy.

For providing Mobile Banking Services through the App, the Bank collects, retains and uses personal information only when it reasonably believes that it is for a lawful purpose and that it will help administer its business or provide products, services, and other opportunities to the visitor/customer. The Bank collects three types of information: personal, sensitive personal data or information and non-personal.

(a) Personal Information

It can be any information that relates to a natural person, which, either directly or indirectly, in combination with other information available is capable of identifying such person. Information including but not limited to name, address, telephone number, e-mail, occupation, etc.

(b) Sensitive Personal Data or Information

The term "Sensitive Personal Data or Information (SPDI)" as per Rule 3 of IT Act 2000 & Amendments (2008) shall mean and include:

Password (Capable of providing information or access to SPDI listed below)

Financial information such as Bank account or Debit Card or other payment instrument details

Physical, Physiological and Mental Health Condition

Sexual Orientation

Any of the detail relating to the above categories of SPDI or information received under above categories of SPDI by the organization for processing, stored or processed under lawful contract or otherwise

4.0 Use of Cookies

Yadrav Co-op Bank Ltd, Yadrav does not use cookies.

Yadrav Co-op Bank Ltd only asks for specific types of personal information. In a few areas on our web site and online customer support tools, we ask you to provide information that will enable us to enhance your site visit, to assist you with technical support issues or to follow up with you after your visit. It is completely optional for you to participate. For example, we request information from you when you:

- Register on yadravbank.in
- Provide feedback in an online survey
- Participate in a sweepstakes or other promotional offer
- Request e-mail notification
- Subscribe to a newsletter or a mailing list
- Request online technical support
- Request assistance from us

In each of the instances above, we may ask for your name, email address, phone number, address, type of business, customer preference information, customer number and service tag number, as well as other similar personal information that is needed to register or subscribe you to services or offers. In the case of newsletters or mailing lists, you will be able to “unsubscribe” to these mailings at any time.

Yadrav Co-op Bank Ltd only uses your personal information for specific purposes. The information you provide will be kept confidential and used to support your relationship with Yadrav Co-op Bank Ltd. Among other things, we want to help you quickly find information on yadravbank.in and alert you to service upgrades, special offers, updated information and other new products and services from Yadrav Co-op Bank Ltd. Agents or contractors of Yadrav Co-op Bank Ltd who have access to your personal information and prospect information are required to keep the information confidential and not use it for any other purpose than to carry out the services they are performing for Yadrav Co-op Bank Ltd. Yadrav Co-op Bank Ltd may enhance or merge your information collected at its site with data from third parties for purposes of marketing products or services to you. You can opt-out of receiving further marketing from Yadrav Co-op Bank Ltd at any time.

We will send you information about our various products and services, or other products and services we feel may be of interest to you. Only Yadrav Co-op Bank Ltd (or agents working on behalf of Yadrav Co-op Bank Ltd and under confidentiality agreements) will send you these direct mailings. If you do not want to receive such mailings, simply tell us when you give us your personal information. Or, at any time you can easily opt-out of receiving further marketing from Yadrav Co-op Bank Ltd by sending us an email at it@yadravbank.com.

Yadrav Co-op Bank Ltd will not disclose your personal information to any outside organization for its use in marketing without your consent.

Information regarding you (such as name, address and phone number) or your order and the products you purchase will not be given or sold to any outside organization for its use in marketing or solicitation without your consent. Your information may be shared with agents or contractors of Yadrav Co-op Bank Ltd for the purpose of performing services for Yadrav Co-op Bank Ltd.

Yadrav Co-op Bank Ltd wants to help you keep your personal information accurate.

You can request the individual information that Yadrav Co-op Bank Ltd has collected about you via the Internet by sending email at it@yadravbank.com. You can have factual inaccuracies in this information corrected by sending us email at it@yadravbank.com.

5.0 Data retention & Deletion

Information provided by you are retained (for later of the) (i) as long as the purposes for which such data were collected continue. Or (ii) for such period so as to satisfy legal, regulatory or accounting requirements or to protect Bank's interests.

The Covered Persons have authorized the Bank to exchange, share, part with all information related to the details and transaction history of the Covered Persons to its Affiliates/ banks / financial institutions / credit bureaus / agencies/participation in any telecommunication or electronic clearing network as may be required by law, customary practice, credit reporting, statistical analysis and credit scoring, verification or risk management or any of the aforesaid purposes and shall not hold The Bank liable for use or disclosure of this information.

As regards the information collected from visitors of the mobile applications, The Bank will use the Information to improve the Covered Person's experience on the site and make subsequent offers to the visitor on products which may be of interest to him / her, if so agreed while giving information.

The data collected from mobile banking customers shall be deleted only after the same is no longer required to provide mobile banking services to the customer or the same is no longer required.

6.0 Data Security

Bank maintains administrative, technical and physical safeguards designed to protect the Confidential Information you provide against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use. In the event your Confidential Information is compromised through no fault by you, Bank shall provide notice to you consistent with state and federal privacy laws. Note: Bank will never ask for you to send your password to them or any other person or bank via an e-mail.

User IDs and Passcodes are used to help safeguard against unauthorized access to your information through the Mobile Banking Application or Mobile Web. As always, we strongly encourage you to assist us in that effort by not sharing your b Banking User ID and Passcodes with anyone.

7.0 Disclosure to Third Parties

Data Subject shall be informed in the privacy notice / SoW / contract agreement, if personal information shall be disclosed to Third Parties / partner firms, and it shall be disclosed only for the purposes described in the privacy notice / SoW / contract agreements and for which the data subject has provided consent.

Personal information of data subjects may be disclosed to the Third Parties / partner firms only for reasons consistent with the purposes identified in the notice / SoW / contract agreements or other purposes authorized by law. Bank shall notify the data subjects prior to disclosing personal information to Third Parties / partner firms for purposes not previously identified in the notice / SoW / contract agreements.

Bank shall communicate the privacy practices, procedures and the requirements for data privacy and protection to the Third Parties / partner firms. The Third Parties shall sign an NDA (Non-Disclosure Agreement) with Bank before any personal information is disclosed to the Third Parties partner firms. The NDA shall include the terms on non-disclosure of customer information. Security Information security policy and procedures shall be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by Bank. Information asset labeling and handling guidelines shall include controls specific to the storage, retention and transfer of personal information.

Management shall establish procedures that maintain the logical and physical security of personal information. Management shall establish procedures that ensure protection of personal information against accidental disclosure due to natural disasters and environmental hazards. Incident response protocols are established and maintained in order to deal with incidents concerning personal data or privacy practices.

8.0 Roles and Responsibilities

The owner for the Privacy Policy shall be the Privacy Officer. the Privacy Officer shall be responsible for maintenance and accuracy of this policy. Any queries regarding the implementation of this Policy shall be directed to the privacy officer. This policy shall be reviewed for updates by Privacy Officer on an annual basis. additionally, the privacy policy shall be updated in-line with any major changes within the organization's operating environment or on recommendations provided by internal/ external auditors.

9.0 Policy Compliance And Review

Compliance to the privacy policy shall be reviewed on an annual basis by Privacy Review Team to ensure continuous compliance monitoring through the implementation of compliance measurements and periodic review processes. For proactive detection of data breaches, please refer breach management policy. In cases where non-compliance is identified, the privacy officer shall review the reasons for such non-compliance along with a plan for remediation and report them to Privacy Review Team.