The Karad Urban Co-Operative Bank Ltd., Karad

Privacy Policy

1. Introduction and Scope

This Privacy Policy ("Policy") outlines how The Karad Urban Co-operative Bank Ltd; Karad ("the Bank," "we," "us," or "our") collects, uses, discloses, stores, secures, and disposes of personal information and sensitive personal data or information (collectively referred to as "Personal Data") entrusted to us by our customers and users. Bank is committed to protecting the privacy and confidentiality of your Personal Data in accordance with the highest standards of data protection and privacy laws. This Policy applies to all Personal Data collected by the Bank through its various channels, including but not limited to its website, mobile applications, online portals, physical branches, and other electronic communications.

This Policy is developed in strict adherence to applicable Indian legal and regulatory frameworks, including the Information Technology Act, 2000 (IT Act), the Digital Personal Data Protection Act, 2023 (DPDPA), relevant provisions of the Indian Penal Code (IPC), and guidelines issued by the Reserve Bank of India (RBI), National Bank for Agriculture and Rural Development (NABARD), Indian Computer Emergency Response Team (CERT-IN) , National Internet Exchange of India (NIXI), and National Payments Corporation of India (NPCI). Furthermore, this Policy integrates globally recognized best practices, particularly those derived from the General Data Protection Regulation (GDPR), to ensure a robust and comprehensive approach to data privacy.

By accessing or using any of Bank's services or platforms, you signify your understanding and acceptance of the terms of this Privacy Policy. We encourage you to read this Policy carefully to understand our practices regarding your Personal Data.

2. Definitions

For the purpose of this Privacy Policy, the following definitions shall apply:

2.1. Personal Data

"Personal Data" 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 Bank, is capable of identifying such person. This includes, but is not limited to:

- Name, address, email address, telephone number
- Date of birth, gender, nationality
- Financial information such as bank account details, credit/debit card numbers, payment instrument details, transaction history

- Identity proofs (e.g., PAN, Aadhaar, Passport details)
- Biometric information (e.g., fingerprints, facial recognition data, if collected)
- Physical, physiological, and mental health condition (if relevant for specific services)
- Sexual orientation (if relevant for specific services)
- Medical records and history (if relevant for specific services)
- Any other information provided to the Bank for availing services.

2.2. Sensitive Personal Data or Information (SPDI)

"Sensitive Personal Data or Information" (SPDI) refers to 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 or otherwise.

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.

2.3. Data Subject

"Data Subject" refers to the natural person whose Personal Data is being collected, processed, or stored by Bank.

2.4. Processing

"Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3. Principles of Data Processing

Bank adheres to the following core principles when processing Personal Data, aligning with both Indian regulations and GDPR principles:

3.1. Lawfulness, Fairness, and Transparency

Personal Data will be processed lawfully, fairly, and in a transparent manner. This means that we will have a legitimate basis for processing your data, we will handle it in a way that is reasonable and expected, and we will clearly inform you about our data processing activities.

3.2. Purpose Limitation

Personal Data will be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. We will only collect data that is necessary for the stated purpose.

3.3. Data Minimization

Personal Data collected will be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed. We will not collect excessive data.

3.4. Accuracy

Personal Data will be accurate and, where necessary, kept up to date. Every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.5. Storage Limitation

Personal Data will be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Once the purpose is fulfilled, the data will be securely disposed of or anonymized, unless retention is required by law.

3.6. Integrity and Confidentiality (Security)

Personal Data will be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures. This includes implementing robust cybersecurity measures as per CERT-IN guidelines and RBI directives.

3.7. Accountability

Bank, as the data controller, is responsible for, and must be able to demonstrate compliance with, the aforementioned principles. We maintain records of our processing activities and have internal policies and procedures to ensure compliance.

4. Collection of Personal Data

Bank collects Personal Data through various means, including:

4.1. Directly from You

We collect Personal Data directly from you when you:

- Apply for our products or services (e.g., opening an account, applying for a loan, credit card)
- Fill out forms, applications, or surveys, whether online or offline
- Interact with our customer service representatives
- Visit our branches
- Participate in promotions, contests, or events
- Provide feedback or make inquiries.

4.2. Through Digital Platforms

When you use our website, mobile applications, or online banking services, we may collect technical and usage data, including:

- IP address, browser type, operating system
- Pages visited, time spent on pages, clickstream data
- Device identifiers, location data (with your consent)
- Information collected through cookies and similar technologies (as detailed in our Cookies Policy).

4.3. From Third Parties

We may receive Personal Data about you from third parties, such as:

- Credit bureaus and other financial institutions for credit assessment and fraud prevention
- Regulatory bodies or law enforcement agencies as required by law
- Service providers who assist us in delivering our products and services.

5. Purpose and Use of Personal Data

Bank collects and uses your Personal Data for the following purposes:

5.1. Providing Products and Services

- To process your applications for banking products and services
- To manage your accounts and provide banking operations
- To facilitate transactions, payments, and fund transfers (in accordance with NPCI protocols)
- To provide customer support and respond to your inquiries.

5.2. Legal and Regulatory Compliance

- To comply with legal and regulatory obligations, including Know Your Customer (KYC) requirements, anti-money laundering (AML) regulations, and counter-terrorism financing (CTF) laws

- To respond to requests from government authorities, law enforcement agencies, or courts
- To prevent, detect, and investigate fraud, cybercrime, and other illegal activities (in line with IT Act and IPC).

5.3. Risk Management and Fraud Prevention

- To assess creditworthiness and manage financial risks
- To detect and prevent fraudulent transactions and unauthorized access to your accounts
- To ensure the security and integrity of our systems and data (as per CERT-IN guidelines.

5.4. Business Operations and Improvement

- To analyze and improve our products, services, and digital platforms
- To conduct internal audits, data analysis, and research
- To personalize your experience and offer tailored products and services
- To conduct marketing and promotional activities (with your consent where required).

5.5. Communication

- To send you important notices, updates, and information about your accounts or services
- To communicate about new products, services, offers, and promotions that may be of interest to you.

6. Disclosure and Sharing of Personal Data

Bank will not disclose or share your Personal Data with any third party except in the following circumstances:

6.1. With Your Consent

We may disclose your Personal Data to third parties if you have provided your explicit consent for such disclosure.

6.2. To Affiliates and Group Companies

We may share your Personal Data with our affiliates and group companies for business operations, service delivery, and internal administrative purposes, provided they adhere to the same standards of data protection as Bank.

6.3. To Service Providers

We may engage third-party service providers to perform functions on our behalf, such as IT services, data processing, marketing, and customer support. These service providers are contractually obligated to protect your Personal Data and use it only for the purposes for which it was disclosed, and in accordance with this Policy and applicable laws.

6.4. For Legal and Regulatory Compliance

We may disclose your Personal Data when required by law, regulation, court order, or governmental request. This includes sharing information with regulatory bodies (e.g., RBI, NABARD), law enforcement agencies, or other authorities to comply with legal obligations or to protect our rights, property, or safety, or the rights, property, or safety of others.

6.5. Business Transfers

In the event of a merger, acquisition, reorganization, or sale of all or a portion of our assets, your Personal Data may be transferred as part of that transaction. We will ensure that the acquiring entity is bound by this Privacy Policy or a similar policy that provides an equivalent level of protection for your Personal Data.

6.6. Aggregated or Anonymized Data

We may share aggregated or anonymized data that does not identify you personally for research, analytical, or statistical purposes.

7. Data Security

Bank is committed to ensuring the security of your Personal Data. We implement robust technical, organizational, and physical security measures to protect your Personal Data from unauthorized access, alteration, disclosure, misuse, loss, or destruction. These measures include:

- **Encryption:** Using encryption technologies for data in transit and at rest where appropriate.
- **Access Controls:** Implementing strict access controls and authentication mechanisms to limit access to Personal Data to authorized personnel only.
- **Network Security:** Employing firewalls, intrusion detection/prevention systems, and other network security tools.
- **Regular Audits and Assessments:** Conducting regular security audits, vulnerability assessments, and penetration testing to identify and address potential weaknesses.
- **Employee Training:** Providing regular training to our employees on data protection, privacy, and information security, best practices.
- **Physical Security:** Maintaining physical safeguards to protect our data centers and physical records.
- **Incident Response Plan:** Having a comprehensive incident response plan to address any data breaches or security incidents promptly and effectively, in accordance with CERT-IN guidelines.

While we strive to protect your Personal Data, no method of transmission over the internet or method of electronic storage is 100% secure. Therefore, we cannot guarantee its absolute security. Users are also responsible for maintaining the confidentiality of their account credentials and for ensuring the security of their own devices.

8. Your Rights

In accordance with applicable data protection laws, including the DPDPA and principles of GDPR, you have certain rights regarding your Personal Data. These rights may include:

8.1. Right to Access

You have the right to request access to the Personal Data we hold about you. Upon request, we will provide you with a copy of your Personal Data, subject to any legal limitations or exemptions.

8.2. Right to Correction/Rectification

You have the right to request the correction or rectification of any inaccurate or incomplete Personal Data we hold about you. We will take reasonable steps to ensure your data is accurate and up to date.

8.3. Right to Erasure (Right to be Forgotten)

In certain circumstances, you may have the right to request the erasure of your Personal Data. This right is not absolute and may be subject to legal obligations or legitimate interests of the Bank (e.g., retention for regulatory compliance).

8.4. Right to Restriction of Processing

You may have the right to request the restriction of processing of your Personal Data in certain situations, such as when you contest the accuracy of the data or when the processing is unlawful.

8.5. Right to Data Portability

Where applicable, you may have the right to receive your Personal Data in a structured, commonly used, and machine-readable format and to transmit that data to another controller.

8.6. Right to Object

You have the right to object to the processing of your Personal Data in certain circumstances, including processing for direct marketing purposes.

8.7. Right to Withdraw Consent

Where processing is based on your consent, you have the right to withdraw your consent at any time. Withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

To exercise any of these rights, please contact our Grievance Redressal Officer or Data Protection Officer.

9. Changes to this Policy

Bank reserves the right to update or modify this Privacy Policy at any time to reflect changes in our practices, technology, legal requirements, or other factors. Any changes will be effective immediately upon posting the revised Policy on our website. We encourage you to review this Policy periodically to stay informed about how we collect, use, and protect your Personal Data. Your continued use of our services or platforms after any modifications to this Policy will constitute your acknowledgment of the modifications and your consent to abide and be bound by the modified Policy.