Karnataka Bank Ltd.
Your Family Bank, Across India.

Regd. & Head Office
P. B. No.599, Mahaveera Circle
Kankanady
Mangaluru – 575 002

Phone : 0824-2228414/179/236
E-Mail : fincell@ktkbank.com
Website : www.karnatakabank.com
CIN : L85110KA1924PLC001128

BRANCH BANKING DEPARTMENT

POLICY ON DATA PRIVACY AND SECURITY FOR AADHAAR ENROLMENT

Table of Contents

1. Introduction:

Karnataka Bank, hereafter referred as Bank, is a Global Authentication User Agency (AUA) and is a KUC User Agency (KUA) license issued by Unique Identification Authority of India (UIDAI). It undertakes user authentications as per the UIDAI guidelines to enable some of its services / business functions. Bank connects to the Central Identities Data Repository (CIDR) through National Payment Corporation of India (NPCI) who is an Authentication Service Agency (ASA/KSA). Bank uses the demographic as well as biometric data in addition to the Aadhaar No/VID of its customers while initiating the account based relationship with its' customers or while providing account based services to the customers.

Since Bank handles sensitive resident information such as the Biometric information, Aadhaar number, e-KYC information etc. of the customers, it becomes imperative to ensure its security and safety to prevent unauthorized access. This Policy is in line with the directions of Information Security Policy issued by UIDAI and is applicable wherever UIDAI information is processed and/or stored by Bank.

2. Objective of the Policy.

The Objective of the Policy include:

2.1 To design suitable controls to ensure the privacy and security of the Biometric information of the customer as well as Aadhaar number and any other data received from the UIDAI in due course of authentication.

2.2 To provide necessary guidelines to enable compliance with Aadhaar Act 2016 and any other applicable circulars or directions issued by the UIDAI.

3. Aadhaar Data Privacy and Security.

3.1 The submission of Aadhaar details by a customer to the Bank is voluntary.

3.2 Bank will not insist on a customer to produce their Aadhaar details for availing any of the services.

3.3 Bank will seek a declaration by the customer for Aadhaar number offered voluntarily by the customer to the Bank.

3.4 Consent will be either in the form of an authorization letter or a provision to electronically record the consent in a software application.

3.5 Biometric details will also be required by the Bank for the purpose of authentication of customer before permitting transaction through Micro ATM/any other device as an AEPS (Aadhaar Enabled Payment System) transaction.

3.6 Bank will use STQC certified devices for capturing biometric data maintained in CIDR against the specific Aadhaar number.

4. Aadhaar Enrolment and Update;

4.1 Regulation 12A of the Aadhaar (Enrolment and Update) Regulation, 2016 mandates the Banks to offer Aadhaar enrolment and updating services.

4.2 These services will be provided at select branches identified by the Bank.

4.3 Aadhaar enrolment and updating entails the process of capturing the personal information of the customers along with their biometric details (Finger print and iris biometrics).

4.4 The data captured at the time of enrolment or updation will be sent to UIDAI as a straight through process. Bank will not store the data captured (both diametric and personal information) in any manner and form.

4.5 UIDAI Rules in respect of Aadhaar enrolment and updation shall be strictly adhered to.

5. Asset Management:

5.1 All assets (business applications, operating systems, databases, network etc.) used for the Aadhaar authentication services shall be identified, labelled and classified.

5.2 Only STQC certified Authentication devices shall be used to capture residents biometric.

5.3 Periodic Vulnerability Assessment (VA) exercise shall be conducted for ensuring the security of the Aadhaar infrastructure and Necessary network intrusion and prevention systems shall be implemented.

5.4 Bank shall implement controls to prevent and detect any loss, damage, theft or compromise of the assets.

6. Information Security Incident Management.

6.1 Bank shall be responsible for reporting any security weakness, any incidents, possible misuse or violation of any stipulated guidelines to UIDAI immediately.

7. Review.

7.1 The Policy will be reviewed once in a year.