
Jio Payments Bank Limited

Privacy Policy

Applicability: Jio Payments Bank Ltd

Issuing Authority: Jio Payments Bank Ltd

Content Owner: Jio Payments Bank Ltd

Policy Custodian: Chief Information Security Officer



Revision History

Version	3.0
Release Date	02/04/2026
Proposed By	Pushkar Sathe
Reviewed By	Saikiran Konchada
Recommended by	Ravi Gali

Purpose of Policy

The purpose of this policy is to provide direction to the various stakeholders and responsible personnel within Jio Payments Bank Limited (JPBL) to protect personal data of Aadhaar number holders in compliance to the relevant provisions of the Aadhaar Act, 2016; the Aadhaar and Other Laws (Amendment) Act, 2019; the Aadhaar (Authentication) Regulations, 2016; the Aadhaar (Data Security) Regulations; the Aadhaar (Sharing of Information) Regulations, 2016; and the Information Technology Act, 2000, and regulations thereunder.

Data Classification & Handling

Data Classification and Handling

JPBL shall classify data based on sensitivity and criticality as follows:

- a. Public Data – Information approved for public disclosure.
- b. Internal Data – Non-sensitive information intended for internal use only.
- c. Confidential Data – Sensitive business or customer information requiring restricted access.
- d. Sensitive Personal Data – Includes Aadhaar number, biometric information, financial information, and any data classified as sensitive under applicable laws.

Handling requirements:

- Access shall be restricted on a need-to-know basis.
- Sensitive Personal Data shall be encrypted at rest and in transit.
- Data handling controls shall be implemented in accordance with classification.

Personal Data collection

Jio Payments Bank Ltd Limited shall collect biometric data Information in addition to Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing Account Opening Services.

Specific purpose for collection of Personal data

- a. The identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide e-KYC services.
- b. The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhaar Act 2016 or its Amendment and Regulations.

c. The identity information shall not be used beyond the mentioned purpose without consent from the Aadhaar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhaar Act 2016.

d. Process shall be implemented to ensure that identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhaar number holder.

Notice / Disclosure of Information to Aadhaar number holder

1. Aadhaar number holders shall be provided relevant information prior to collection of identity information personal data. These shall include:

- a. The purpose for which personal data / identity information is being collected;
- b. The information that shall be returned by UIDAI upon authentication;
- c. The information that the submission of Aadhaar number or the proof of Aadhaar is mandatory or voluntary for the specified purpose and if mandatory the legal provision mandating it;
- d. The information that Virtual ID can be used in lieu of an Aadhaar number at the time of Authentication.

2. Aadhaar number holder shall be notified of the authentication either through the e-mail or phone or SMS at the time of authentication and the JPBL shall maintain logs of the same;

Obtaining Consent

a. Upon notice / disclosure of information to the Aadhaar number holder, consent shall be taken in electronic form or any other appropriate means.

b. JPBL Limited shall maintain logs of disclosure of information and Aadhaar number holder's consent.

c. The legal department shall be involved in vetting the method of taking consent and logging of the same, and formal approval shall be recorded from the legal department.

Processing of Personal data

a. The identity information, including Aadhaar number, biometric /demographic information collected from the Aadhaar number holder by JPBL shall only be used for the Aadhaar authentication process by submitting it to the Central Identities Data Repository (CIDR).

- b.** Aadhaar authentication or Aadhaar e-KYC shall be used for the specific purposes declared to UIDAI and permitted by UIDAI. Such specific purposes shall be notified to the residents / customers / Individuals at the time of authentication through disclosure of information notice.
- c.** JPBL Limited shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under Aadhaar Act 2016 and its associated Regulation and informed to the resident / customers / individuals at the time of Authentication.
- d.** For the purpose of e-KYC, the demographic details of the individual received from UIDAI as a response shall be used for identification of the individual for the specific purposes of providing the specific services for the duration of the services.

Retention of Personal Data & Secure Deletion

Personal data shall be retained only for as long as necessary to fulfill the purpose of processing or as required by applicable laws and regulations. The authentication logs, consent records, and audit trails shall be retained as per regulatory requirements including UIDAI, RBI, and applicable laws.

Furthermore, the authentication transaction logs shall be stored for a period of two years subsequent to which the logs shall be archived for a period of five years or as per the regulations governing the entity, whichever is later and upon expiry of which period, barring the authentication transaction logs required to be maintained by a court order or pending dispute, the authentication transaction logs shall be deleted.

Upon expiry of retention period, data shall be securely deleted using approved methods such as cryptographic erasure or anonymization. Periodic review shall be conducted to ensure compliance with retention and deletion requirements.

Sharing of Personal data

- a.** Identity information shall not be shared in contravention to the Aadhaar Act 2016, its Amendment, Regulations and other circulars released by UIDAI from time to time.
- b.** Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhaar Act and regulations.

Data Security

- a.** The Aadhaar number shall be collected over a secure application, transmitted over a secure channel as per specifications of UIDAI and the identity information returned by UIDAI shall be stored securely; **b)** The biometric information shall be collected, if applicable, using

- b.** The Aadhaar number shall be collected over a secure application, transmitted over a secure channel as per specifications of UIDAI and the identity information returned by UIDAI shall be stored securely; b) The biometric information shall be collected, if applicable, using the registered devices specified by UIDAI. These devices encrypt the biometric information at device level and the application sends the same over a secure channel to UIDAI for authentication.
- c.** OTP information shall be collected in a secure application and encrypted on the client device before transmitting it over a secure channel as per UIDAI specifications;
- d.** Aadhaar/VID number that are submitted by the resident/ customer/ individual to the requesting entity and PID block hence created shall not be retained under any event and JPBL shall retain the parameters received in response from UIDAI;
- e.** e-KYC information shall be stored in an encrypted form only. Such encryption shall match UIDAI encryption standards and follow the latest Industry best practice;
- f.** JPBL shall, as mandated by law, encrypt and store the Aadhaar numbers and any connected data only on the secure Aadhaar Data Vault (ADV) in compliance to the Aadhaar data vault circular issued by UIDAI; g) The keys used to digitally sign the authentication request and for encryption of Aadhaar numbers in Data vault shall be stored only in HSMs in compliance to the HSM and Aadhaar Data vault circulars; h) JPBL shall use only Standardization Testing and Quality Certification (STQC) / UIDAI certified biometric devices for Aadhaar authentication (if biometric authentication is used).
- g.** All applications used for Aadhaar authentication or e-KYC shall be tested for compliance to Aadhaar Act 2016 before being deployed in production and after every change that impacts the processing of Identity information; The applications shall be audited on an annual basis by information systems auditor(s) certified by STQC, CERT-IN or any other UIDAI recognized body.
- h.** Personal Data Breach Notification and Management
 - a.** Any breach involving personal data, including Aadhaar-related information, shall be promptly identified, reported, and managed.
 - b.** JPBL shall notify UIDAI, CERT-In, RBI, and other regulatory authorities as applicable within prescribed timelines.
 - c.** An internal escalation matrix involving CISO, Legal, and Senior Management shall be followed.
 - d.** Root cause analysis and corrective actions shall be implemented and documented.

Furthermore, In the event of an identity information breach, the organization shall notify UIDAI of the following:

- Any confidentiality breach/security breach of Aadhaar related information shall be reported to UIDAI within 24 hours;
 - A description and the consequences of the breach;
 - A description of the number of Aadhaar number holders affected and the number of records affected;
 - UIDAI Technical SPOC contact details;
 - Measures taken to mitigate the identity information breach.
- i. Appropriate security and confidentiality obligations shall be implemented in the non-disclosure agreements (NDAs) with employees/contractual agencies /consultants/advisors and other personnel handling identity information.
- j. Only authorized individuals shall be allowed to access Authentication application, audit logs, authentication servers, application, source code, information security infrastructure. An access control list shall be maintained and regularly updated by organization;
- k. Best practices in data privacy and data protection based on international Standards shall be adopted;
- l. The response received from CIDR in the form of authentication transaction logs shall be stored with following details:
- The Aadhaar number against which authentication is sought. In case of Local AUAs where Aadhaar number is not returned by UIDAI and storage is not permitted, respective UID token shall be stored in place of Aadhaar number;
 - Specified parameters received as authentication response;
 - The record of disclosure of information to the Aadhaar number holder at the time of authentication;
 - Record of consent of the Aadhaar number holder for authentication but shall not, in any event, retain the PID information.
- m. Aadhaar numbers shall only be stored in Aadhaar Data vault as per the specifications provided by UIDAI.

Privacy by Design & Default

- a. Processes shall be established to embed privacy aspects at the design stage of any new systems, products, processes and technologies involving data processing of identity information of Aadhaar number holders;
- b. JPBL in possession of the Aadhaar number of Aadhaar number holders, shall not make public any database or records of the Aadhaar numbers unless the

- Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and in electronic form;
- c. Before going live with any new process that involves processing of identity information, JPBL shall ensure that disclosure of information / privacy notice in compliance to the Aadhaar Act 2016 is provided to the resident / customer / individual and that consent is taken and recorded in compliance to Aadhaar Act 2016;
 - d. Quarterly self-assessments shall be conducted to ensure compliance to disclosure of information and consent requirements;
 - e. Privacy enhancing organizational and technical measures like anonymization, de-identification and minimization shall be implemented to make the collection of identity information adequate, relevant, and limited to the purpose of processing.
 - f. Privacy considerations shall be embedded into the design of all systems, applications, and processes involving personal data.
 - g. By default, only minimum necessary personal data shall be collected and processed.
 - h. Default settings shall ensure maximum privacy protection unless explicitly modified by the user.
 - i. Periodic privacy impact assessments shall be conducted for new and existing Systems.

Governance Structure

Governance and Roles & Responsibilities

- a. JPBL shall establish a governance framework for personal data protection.
- b. Key roles shall include:
 - Chief Information Security Officer (CISO)
 - Business/Data Owners
 - IT/System Owners
- c. A Data Privacy or Information Security Committee shall oversee implementation and compliance.
- d. The policy shall be reviewed at least annually or upon regulatory changes.

Logging, Monitoring & Audit

- a. All access to personal data, including Aadhaar-related systems, shall be logged and monitored.

- b. Logs shall be stored securely and protected against tampering.
- c. Centralized monitoring systems (e.g., SIEM) shall be used for detecting anomalies.
- d. Periodic internal and external audits shall be conducted to ensure compliance.

Rights of the Aadhaar Number Holder

- a. The Aadhaar number holder has the right to obtain and request update of identity information stored with the organization, including authentication logs. The collection of core biometric information, storage and further sharing is protected by Section 29 of the Aadhaar Act 2016, Hence the Aadhaar number holder cannot request for the core biometric information.
- b. JPBL shall provide a process for the Aadhaar number holder to view their identity information stored and request subsequent updation after authenticating the identity of the Aadhaar number holder. In case the update is required from UIDAI, the same shall be informed to the Aadhaar number holder.
- c. The Aadhaar number holder may, at any time, revoke consent given to JPBL for storing his e-KYC data, and upon such revocation, JPBL shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.
- d. The Aadhaar number holder has the right to lodge a complaint with the Grievance officer who is responsible for monitoring of the identity information processing activities so that the processing is not in contravention of the law.

Grievance Redressal Mechanism

- a. Aadhaar number holders with grievances about the processing can contact the organization's Grievance Officer via multiple channels like on the website, through phone, SMS, mobile application.
- b. The contact details of Grievance Officer and the format for filing the complaint shall be displayed on the organization's website and other such mediums that are commonly used for interaction with the residents / customers / individuals;

Relevant Provisions of Aadhaar Act and Supreme court judgement

JPBL shall refer to the following documents for ensuring compliance to the Aadhaar requirements:

- a. Aadhaar Act 2016
- b. Aadhaar (Authentication) Regulations 2016



- c. Aadhaar (Data Security) Regulations 2016
- d. Aadhaar (Sharing of Information) Regulations 2016
- e. UIDAI Information Security Policy for AUA/KUA
- f. Various circulars issued by UIDAI.