Aadhaar Privacy Policy

DOCUMENT CLASSIFICATION	Public
DOCUMENT REF	MML-APP-I-001
VERSION	1.0
DATED	25 March 2024
DOCUMENT OWNER	IT Department
APPROVED BY	The Board of Directors

Revision History

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES
1.0	25 March 2024	IT	New policy

Distribution

NAME	TITLE
ISSG	Information Security Steering Committee

Table of Contents

1 Introduction

The purpose of this document is to set out the organization's policy regarding privacy of Aadhaar data collected, stored, and processed by MML. MML recognizes the security of UIDAI information in line with the Aadhaar Act 2016. The confidentiality, integrity, and availability of these shall be always maintained by MML and its partners by deploying security controls in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards.

2 Aadhaar Privacy Policy

2.1 Objective & Purpose

To provide a framework of rules / regulations / standards / practices to the Aadhaar Privacy Policy to ensure that same are in line with the Aadhaar Act 2016, Aadhaar Authentication Application Security Standards. This policy outlines the Information Security Policy and Information Security Controls applicable to MML acting as Authentication User Agency (AUA)/KYC User Agency (KUA).

MML shall ensure the security of UIDAI information assets by:

- Providing an approach and directives for deploying security controls for all information assets used for providing authentication services.
- Establishing review mechanism to ensure that the MML adhere to all provisions of the UIDAI Information Security Policy for AUAs/KUAs.

2.2 Coverage

This policy covers the following broad areas which help establish, govern, and manage Aadhaar Privacy Policy as directed by UIDAI on the basis of following regulations.

- Aadhaar Regulations 2016
- Aadhaar (Authentication and Offline Verification) Regulations 2021

2.3 Scope

- 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.

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

2.4 Applicability

The policy will apply to all departments/employees of MML that access, process, or store Aadhaar number and any other data received from the customers or UIDAI in due course of authentication.

2.5 Review

Aadhaar Privacy Policy shall be reviewed once in Two years or earlier, in the event of significant changes occur to ensure its continuing suitability, adequacy, effectiveness and regulatory compliances. Procedures and Processes will be reviewed and updated accordingly.

2.6 Approval

Aadhaar Privacy Policy and its updates shall be placed by IT to the ISSG / the Board of Directors.

2.7 Compliance

- Enforcement of the Aadhaar Privacy Policy shall be mandatory.
- Compliance with Aadhaar Privacy Policy is mandatory for all applicants as per applicability.
- MML shall not reproduce the name and logo of “Aadhaar” without authorization of UIDAI.
- MML shall use “Aadhaar” logo/name during the term of agreement with UIDAI for authentication service without any modification.
- MML shall not authorize any other entity to use “Aadhaar” name and logo without permission from UIDAI.

2.8 Exception

Dispensation to be sought from ISSG for any deviations to the Aadhaar Privacy Policy based on adequate business justification and recommendation / approval by respective Business Head / Function Head, unless otherwise specified in this policy.

3 Policy

3.1 Introduction

- The Unique Identification Authority of India has been established by the Government of India with the mandate to the Authority to issue unique identification number (called Aadhaar ID 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 establish their identity easily and effectively, 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 registered mobile phone or e-mail address.

3.2 Definition

- **Authentication User Agencies (AUA)**: Authentication User Agency is an organisation or an entity using AADHAAR authentication as part of its applications to provide services to residents.
- **KYC User Agencies (KUA)**: KYC User Agency is an organisation or an entity using AADHAAR authentication and eKYC services from UIDAI as part of its applications to provide services to residents.

3.3 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 based on 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 to supply services and give access to benefits.
- e-KYC Service: UIDAI also provides the e-KYC service, which enables a resident having an Aadhaar number to share their demographic information (i.e., Name, Address, Date of Birth, Gender, Phone & E-mail) and Photograph with UIDAI partner organization (called a KYC User Agency – KUA) in an online, secure, auditable manner with the resident's consent. The consent by the resident can be given via a Biometric authentication or One Time Password (OTP) authentication.
- MML shall collect Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing the services.
- MML has entered into a formal agreement with UIDAI to access Aadhaar authentication services, and e-KYC services. To protect the Aadhaar Beneficiary, the Aadhaar privacy policy of MML has been defined and formulated.

3.4 Data Privacy on Aadhaar and Biometric details

- The submission of Aadhaar details by a customer to MML is voluntary and MML shall 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 MML, MML shall seek a declaration by the customer towards the same.
- Aadhaar numbers collected through physical forms or photocopies of Aadhaar letters shall be masked by redacting the first 8 digits of the Aadhaar number before storing the physical copies.
- Where customers are not willing to provide Aadhaar number for authentication, MML shall provide alternative authentication mechanism to customers for availing the services.
- Virtual ID can be used in lieu of Aadhaar number at the time of Authentication.
- For cases where e-KYC verification is required, MML shall get an explicit consent from the resident for download of details from UIDAI mentioning the purpose for which the details are sought.
- The consent shall be either in the form of an authorization letter or a provision to electronically record the consent in a software application and MML shall maintain logs of disclosure of information and Aadhaar number holder's consent.
- Biometric details shall also be captured by MML for the purposes of authentication, for example, to authenticate a customer for providing services.
- The biometric details whenever captured by MML shall 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.
- Aadhaar number holder shall be notified of the authentication either through the e-mail or phone or SMS at the time of authentication and MML shall maintain logs of the same.
- MML shall use STQC-certified devices and demographic details received from UIDAI shall be stored for future reference.

3.5 Asset Management

Authentication devices used to capture customer biometric should be STQC certified as specified by UIDAI.

3.6 Access Control

The local security settings on all the systems shall be aligned and synced with the Active Directory or similar solutions.

3.7 Password Policy

The password policy is applicable as per our Information Security Policy.

3.8 Cryptography

- The Personal Identity data (PID) block comprising of the customer's demographic / biometric data shall be encrypted as per the latest API documents specified by the UIDAI.
- The PID shall be encrypted during transit and flow within the authentication ecosystem.
- While establishing a secure channel to the AADHAAR Authentication Server (MML shall verify the following:
    - The digital certificate presented has been issued / signed by a trusted Certifying Authority (CA).
    - The digital certificate presented has neither been revoked nor expired.
    - The Common Name (CN) on the certificate presented matches with its fully qualified domain name (presently, auth.uidai.gov.in).
- HSM shall be deployed to store the encryption keys with restricted access, periodic reviews and FIPS 140 standard.

3.9 Physical and Environmental Security

- MML servers involved in Aadhaar authentication mechanism should be placed in a secure lockable cage in the Data Centre.
- The facility should be manned by security guards during and after office hours.
- CCTV surveillance shall cover the data centres where Aadhaar data is processed.

3.10 Sharing of Personal data

- 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.
- Biometric information collected shall not be transmitted over any network without creation of encrypted PID block as per Aadhaar Act and regulations.

3.11 Data Security

- The Aadhaar numbers shall be collected over a secure application, transmitted over a secure channel as per the specifications of UIDAI and the identity information returned by UIDAI shall be stored securely.
- The biometric information shall be collected, if applicable, using the registered devices specified by UIDAI. These devices encrypt the biometric information at the device level and the application sends the same over a secure channel to UIDAI for authentication.
- 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.

- 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 entity shall retain the parameters received in response from UIDAI.
- The keys used to digitally sign the authentication request and for encryption of Aadhaar numbers in Data vault shall be stored only in HSMs.
- MML shall use only Standardisation Testing and Quality Certification (STQC) / UIDAI certified biometric devices for Aadhaar authentication (if biometric authentication is used).
- 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.
- USB, Internet, and privileged account usage will be restricted in the applicable infrastructure.
- Access rights and privileges to information processing facilities for Aadhaar related information shall be revoked within 24 hours of exit of respective personnel. Post deactivation, user IDs shall be deleted if not in use.
- Segregation of duties for personnel involved in operational, development, testing, administration, monitoring etc. shall be implemented for ensuring data security.
- In the event of an identity information breach, the organisation shall notify UIDAI of the following:
    - A description and the consequences of the breach.
    - A description of the number of Aadhaar number holders affected and the number of records affected.
    - The single point contact details.
    - Measures taken to mitigate the identity information breach.
- Organization would inform UIDAI without delay within 72 hours after having knowledge of misuse of any information related to the Aadhaar-related information or system, or compromise of Aadhaar-related information.
- 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.
- MML shall inform UIDAI regarding any unauthorized use or misuse of “Aadhaar” name/ logo and provide necessary assistance to protect the rights of UIDAI including IPR in respect of “Aadhaar” name and logo.
- The response received from CIDR in the form of authentication transaction logs shall be stored with following details:
    - 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.

3.12 Processing of personal data

- The identity information, including Aadhaar number, biometric /demographic information collected from the Aadhaar number holder by MML shall only be used for the Aadhaar authentication process by submitting it to the Central Identities Data Repository (CIDR).
- 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 customers / Individuals at the time of authentication through disclosure of information notice.
- MML shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under applicable laws prevalent in India from time to time and informed to the resident / customers / individuals at the time of Authentication.
- 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.

3.13 Specific purpose for collecting Personal Data

- The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder.
- 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.
- 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.
- MML shall ensure that Identity information is not used beyond the purposes mentioned in the notice/consent form provided to the Aadhaar number holder.

3.14 Operations Security

- Periodic VA exercises should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.

- MML shall ensure that necessary Secure Software Development Life Cycle is followed for software involved in authentication services.
- MLL shall not intentionally write, generate, compile, copy, or attempt to introduce any computer code designed to damage or otherwise hinder the performance of, or access to, any PID information.
- All hosts that connect to the AADHAAR Authentication Service or handle resident's identity information shall be secured using endpoint security solutions. At the minimum, anti-virus / malware detection software shall be installed on such hosts.
- Necessary security systems for infrastructure should be in place – e.g., Firewall, EDR, etc.
- The equipment used by MML will be hardened by enforcing security policies and endpoint security wherever applicable.
- MML shall ensure that the event logs recording the critical user activities, exceptions and security events shall be enabled and stored to assist in future investigations and access control monitoring.
- Regular monitoring of the audit logs shall take place and access to audit trails and event logs shall be provided to authorized personnel only.
- The authentication audit logs should contain, but not limited to, the following transactional details:
    - Reference identity against which authentication is sought.
    - Specified parameters of authentication request submitted.
    - Specified parameters received as authentication response.
    - The record of disclosure of information to the Aadhaar number holder at the time of authentication
    - Record of the consent of Aadhaar number holder for the resident
    - Details of the authentication transaction such as API Name, AUA / KUA Code, Transaction ID, Timestamp, Response Code, Response Timestamp, and any other non-id entity information.
- Logs shall not, in any event, retain the PID, biometric and OTP information.
- No biometric data pertaining to the customer shall be stored within the terminal device.
- The logs of authentication transactions shall be maintained by MML for a period of 2 years, during which an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.
- Upon expiry of the period of 2 years, the logs shall be archived for a period of 5 years, or the number of years as required by the laws or regulations governing MML, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by court or for any pending disputes.
- All system clocks shall be set to an agreed standard using a NTP server or must be managed centrally and procedure shall be made to check for and correct any significant variation.

- Server dedicated for the Online AADHAAR Authentication purposes shall not be used for any other activities.
- Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhaar Act and its Regulations.

3.15 Regulatory References

- Aadhaar Act 2016
- Requesting Entity Compliance Checklist_v_3.0
- Aadhaar (Authentication and Offline Verification) Regulations, 2021
- UIDAI Information Security Policy for AUA/KUA
- Various circulars issued by UIDAI.

3.16 Grievance Redressal

- Aadhaar number holders with grievances about the processing can contact the organisation's grievance redressal forum via multiple channels like through website, phone/toll free number, email etc.
- The detailed grievance address mechanism is published in MML's website, https://muthootmicrofin.com/grievance-redressal-mechanism/
- If issues are not resolved through grievance mechanism, Aadhaar number holders can seek redressal by way of mechanisms as specified in Section 33B of the Aadhaar Act, 2016.

3.17 Glossary

Short Code	Abbreviation
KYC	Know Your Customer
ISSG	Information Security Steering Group
AUA	Authentication User Agency
ASA	Authentication Service Agency
CIDR	Central Identities Data Repository
KUA	Know your customer User Agencies
OTP	One Time Password
PID	Personal Identity Data
STQC	Standardisation Testing and Quality Certification Directorate


muthoot
MICROFIN