Information Security (Personal Data)

Policy for protection of personal data of Aadhar Number holders

2024

Enterprise-wide applicable

Document Information

S No	Item	Description
1	Document Title	Information Security (Personal Data - UIDAI & Aadhar) - Policy for protection of personal data of Aadhar Number holders
2	Document Version	1.0
3	Validity Period	Until renewal (renew every 12 months)
4	Document Owner	Patanjali Somayaji (CTO)

Review Log

No	Item	Name	Date
1	Prepared by	Patanjali Somayaji	10 Apr 2024
2	Reviewed & recommended by	Sashank Rishyasinga	31 Apr 2024
3	Approvals	Technology Strategy Committee & Board Approved	05 Jun 2024

Version History / Change Log

Version	Date Issued	Brief summary of change	Owner's Name
V1.0	10 Apr 2024	Initial Version of Policy	Patanjali Somayaji

1. Introduction

This policy is an additional Information Security policy document, specific to the usage and protection of personal information of Aadhar Number holders.

The purpose of this policy is to provide direction to the various stakeholders and responsible personnel within Axio 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.

This policy applies to all employees, contractors, and third-party service providers involved in the above activities.

The overall responsibility of (1) monitoring and enforcement of this policy through various mechanisms such as Audits etc, (2) implementation of controls of this policy shall be with Head, Compliance and (3) Disclosure of information notice, consent clause, method of consent, logging of consent etc. shall be with Head, Compliance.

2. Personal Data Collection

Data collection

Axio shall collect the personal data including Aadhaar number/Virtual ID, directly from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing the services;

Specific purpose for collection

- The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide e-KYC for Account opening .
- 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.
- cThe 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.
- 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 Aadhar Number holder

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

- The purpose for which personal data / identity information is being collected;
- The information that shall be returned by UIDAI upon authentication;
- 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;
- The alternatives to submission of identity information (if applicable);
- Details of Section 7 notification (if applicable) by the respective department under the Aadhaar Act, 2016, which makes submission of Aadhaar number as a mandatory or necessary condition to receive subsidy, benefit or services where the expenditure is incurred from the Consolidated Fund of India or Consolidated Fund of State. Alternate and viable means of identification for delivery of the subsidy, benefit or service may be provided if an Aadhaar number is not assigned to an individual;
- The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication;
- The name and address of Axio, collecting and processing the personal data;

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

Obtaining consent

- Upon notice / disclosure of information to the Aadhaar number holder, consent shall be taken in writing or in electronic form on the website or mobile application or other appropriate means and Axio shall maintain

logs of disclosure of information and Aadhaar number holder's consent.

- 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

- The identity information, including Aadhaar number, biometric /demographic information collected from the Aadhaar number holder by Axio 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 residents / customers / Individuals at the time of authentication through disclosure of information notice;
- Axio shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under <Specific applicable law to be mentioned by the requesting entity> 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 for the duration of the services.

Retention of personal data

Authentication logs shall be maintained by Axio for a period of 2 (two) years, during which period the Authority and/or the requesting entity may require access to such records for grievance redressal, dispute redressal and audit in accordance with the procedure specified in these regulations.

Upon expiry of the period specified in sub-regulation (2), the authentication logs shall be archived for a period of five years, and upon expiry of the said period of five years or the number of years as required by the laws or regulations governing the entity whichever is later, the authentication logs shall be deleted except those logs required to be retained by a court or which are required to be retained for any pending disputes.

Authentication transaction data shall be retained by the Authority for a period of 6 months, and thereafter archived for a period of five years.

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;
- Axio shall not require an individual to transmit the Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances;

3. Data Security

- 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;
- 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.
- 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;
- 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;
- Axio has been classified as a Local AUA by UIDAI and does not store Aadhaar numbers of the customers / individuals / residents to maintain their privacy and security;
- 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;
- Axio 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;
- 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 privacy officer's contact details;
    - Measures taken to mitigate the identity information breach;
- 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;
- 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 organisation;
- Best practices in data privacy and data protection based on international Standards shall be adopted;
- 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; and
    - Record of consent of the Aadhaar number holder for authentication but shall not, in any event, retain the PID information.
- An Information Security policy in-line with ISO27001 standard, UIDAI specific Information Security policy and Aadhaar Act 2016 shall be formulated to ensure Security of Identity information.
- Aadhaar numbers shall only be stored in Aadhaar Data vault as per the specifications provided by UIDAI.
- Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhaar Act and its Regulations.

4. Rights of the Aadhar Number Holder

- The Aadhaar number holder has the right to obtain and request update of identity information stored with the organisation, 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.
- Axio 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, same shall be informed to the Aadhaar number holder.
- The Aadhaar number holder may, at any time, revoke consent given to Axio for storing his e-KYC data, and upon such revocation, Axio shall delete the e-KYC data in a verifiable manner and provide an acknowledgement of the same to the Aadhaar number holder.
- The Aadhaar number holder has the right to lodge a complaint with the privacy officer who is responsible for monitoring of the identity information processing activities so that the processing is not in contravention of the law;

5. Aadhar Number Holder access request

- A process shall be formulated to handle the queries and process the exercise of rights of Aadhaar number holders with respect to their identity information / personal data. As part of the process it shall be mandatory to authenticate the identity of the Aadhaar number holder before providing access to any identity information.
- All requests from the Aadhaar number holder shall be formally recorded and responded to within a reasonable period.
- Compliance to the relevant data protection / privacy law (s) shall be ensured.

6. Privacy by design

- 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;
- Axio, 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;
- Before going live with any new process that involves processing of identity information, the organisation 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.
- Quarterly self-assessments shall be conducted to ensure compliance to disclosure of information and consent requirements
- 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.

7. Governance and accountability obligations

- Privacy committee shall be established to provide strategic direction on Privacy matters
- A person (Privacy Officer) responsible for developing, implementing, maintaining and monitoring the comprehensive, organization-wide governance and accountability shall be designated to ensure compliance with the applicable laws.
- The name of the Privacy Officer and contact details shall be made available to UIDAI and other external agencies through appropriate channel;
- The Privacy Officer shall be responsible to assess privacy risks of processing Identity information / personal data and mitigate the risks;
- The Privacy Officer shall be independent and shall be involved in all the issues relating to processing of identity information;
- The Privacy Officer shall be an expert in data protection and privacy legislations, regulations and best practices;
- The Privacy Officer shall advise the top management on the privacy obligations;
- The Privacy Officer shall advise on high-risk processing and the requirement of data privacy impact assessments;

- The Privacy Officer shall act as a point of contact for UIDAI for coordination and implementation of privacy practices and other external agencies for any queries;
- The Privacy Officer shall be responsible for managing privacy incidents and responding to the same;
- The Privacy Officer shall also be responsible for putting in place measures to create awareness and training of staff involved in processing identity information, about the legal consequences of data breach to the reputation of the organization;
- Privacy officer shall ensure that the Authentication operations, systems and applications are audited by CERT-IN (Indian Computer Emergency Response Team), Standardisation Testing and Quality Certification (STQC) empanelled auditors or any other UIDAI recognised body atleast on an annual basis;
- Privacy officer shall conduct internal audits (through internal audit team) on a quarterly basis and monitor compliance through these audits against Aadhaar Act 2016;
- Privacy officer shall ensure that the front-end operators interacting with Aadhaar number holders are trained on a periodic basis to ensure they communicate the disclosure of information to the Aadhaar number holder, take consent appropriately after showing the screen to the Aadhaar number holder and ensure Security of identity information. Such trainings shall be documented for audit purposes;
- Aadhaar specific trainings to developers, systems admins and other users shall be provided to ensure they are aware of the obligations for their respective roles; Completion of such trainings shall be documented;
- Privacy officer shall be responsible to formally communicate this policy to all stakeholders and staff who need to comply with this policy; Any changes to the policy shall be communicated immediately;
- Privacy Officer shall facilitate formal Privacy performance reviews with the relevant stakeholders / Privacy Committee and suggest improvements. The reviews shall consider the results of various audits, privacy incidents, privacy initiatives, UIDAI requirements etc.

8. Grievance redressal mechanism

- Aadhaar number holders with grievances about the processing can contact the organisation's Privacy Officer via multiple channels like on the website, through phone, SMS, mobile application etc.

- Reasonable measures shall be taken to inform the residents / customers / individuals about the Privacy Officer and its contact details;
- The contact details of Privacy Officer and the format for filing the complaint shall be displayed on the organisations' website and other such mediums that are commonly used for interaction with the residents / customers / individuals;
- Where the medium of interaction is not electronic (such as physical), Poster / Notice board that is prominently visible shall be used to display the name of Privacy officer and contact details;
- If any issue is not resolved through consultation with the management of Axio, Aadhaar number holders can seek redressal by way of mechanisms as specified in Section 33B of the Aadhaar Act, 2016.

9. Terms and definitions

- "Aadhaar number" means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section.

  Reference: Section 2(a) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and Section 3(i)(a) of the Aadhaar and Other Laws (Amendment) Act, 2019

- "Aadhaar Data Vault" (ADV) means a separate secure database/vault/system where the entities mandatorily store Aadhaar numbers and any connected data such that it will be the only place where the said data will be stored.

  Reference: Point number (a) Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25.07.2017

- "Anonymization" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which an individual cannot be identified, which meets the standards of irreversibility.

  Reference: Section 3 (2) of the Personal Data Protection Bill 2019

- "Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its

verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it.

Reference: Section 2(c) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "Authentication Service Agency" or "ASA" shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority.

  Reference: Regulation number 2(f) of the Aadhaar (Authentication) Regulations, 2016

- "Authentication User Agency" or "AUA" means a requesting entity that uses the Yes/ No authentication facility provided by the Authority.

  Reference: Regulation number 2(g) of the Aadhaar (Authentication) Regulations, 2016

- "Authority" means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

  Reference: Section 2(e) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "Biometric information" means photograph, fingerprint, iris scan, or such other biological attributes of an individual as may be specified by regulations.

  Reference: Section 2(g) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "Central Identities Data Repository" (CIDR) means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto.

  Reference: Section 2(h) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "Consent" means the consent referred to in section 11 of PDP bill 2019
- Reference: section 11 of PDP bill 2019 (given below)
    - (1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

- (2) The consent of the data principal shall not be valid, unless such consent is—
  - (a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;
  - (b) informed, having regard to whether the data principal has been provided with the information required under section 7;
  - (c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose of processing;
  - (d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and
  - (e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.
- (3) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—
  - (a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;
  - (b) in clear terms without recourse to inference from conduct in a context; and
  - (c) after giving him the choice of separately consenting to the purposes of, operations in, the use of different categories of, sensitive personal data relevant to processing.
- (4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.
- (5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.
- (6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal.

- “De-identification” means the process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;

Reference: Section 3(16) of the Personal Data Protection bill 2019

- "Demographic information" includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history.

  Reference: Section 2(k) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "e-KYC User Agency" or "KUA" shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority.

  Reference: Regulation number 2(l) of the Aadhaar (Authentication) Regulations, 2016

- "Local AUAs" means the agencies which will only have access to Limited KYC and will not be allowed to store Aadhaar number within their systems.

  Reference: Point number 9(b) of Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

- "Hardware Security Module (HSM)" means a device that will store the keys used for digital signing of Auth XML and decryption of e-KYC response data received from UIDAI.

  Reference: Point number 4 of Circular No. 11020/204/2017 – UIDAI (Auth-I), dated 22.06.2017

- "Identity information" in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information.

  Reference: Section 2(n) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- "Limited KYC" means the service that does not return Aadhaar number and only provides an agency specific unique UID Token along with other demographic fields that are shared with the Local AUAs depending upon its need.

  Reference: Point number 3 (II) and 9(b) of – Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

- "PID Block" means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication.

  Reference: Regulation number 2(n) of the Aadhaar (Authentication) Regulations, 2016

- “Personal data” means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;

  Reference: Section 3(28) of the Personal Data Protection bill 2019

- “Personnel” means all the employees, staff and other individuals employed/contracted by the requesting entities;

  Reference: Regulation number 2 (1) (f) of Aadhaar (Data Security) Regulations 2016

- "Processing" in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

  Reference: Section 3(31) of the Personal Data Protection bill 2019

- “Reference Key” means an additional key which is mapped with each Aadhaar number stored in the Aadhaar data vault.

  Reference: Point number (c) Circular No. 11020/205/2017 – UIDAI (Auth-I), dated 25.07.2017

- “Requesting Entity” means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication.

  Reference: Section 2(u) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- “Resident” means an individual who has resided in India for a period or periods amounting in all to one hundred and eighty-two days or more in the twelve months immediately preceding the date of application for enrolment.

  Reference: Section 2(v) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016

- “Sensitive personal data or information” means such personal information which consists of information relating to —
  - i. password;
  - ii. financial information such as Bank account or credit card or debit card or other payment instrument details;

- iii. physical, physiological and mental health condition;
- iv. sexual orientation;
- v. medical records and history;
- vi. Biometric information;
- vii. any detail relating to the above clauses as provided to body corporate for providing service; and
- viii. 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 these rules.

Reference: Rule 3 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

- "UID Token" means a 72-character alphanumeric string returned by UIDAI in response to the authentication and Limited KYC request. It will be unique for each Aadhaar number for a particular entity (AUA/Sub-AUA) and will remain same for an Aadhaar number for all authentication requests by that particular entity.

  Reference: Point number 10 of in Circular No. 1 of 2018, F. No. K-11020/217/2018-UIDAI (Auth-I), dated 10th January 2018

- "Virtual ID (VID)" means any alternative virtual identity issued as an alternative to the actual Aadhaar number of an individual that shall be generated by the Authority in such manner as may be specified by regulations.

  Reference: Section 3 (4) of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and Section 4 of the Aadhaar and Other Laws (Amendment) Act, 2019

10. Relevant Provisions

Relevant provisions of the Aadhar Act and Supreme Court judgement are referenced below. These documents shall be referred to for ensuring compliance to the Aadhar requirements:

- Judgement of Honorable Supreme court dated September 2018
- Aadhaar Act 2016
- Aadhaar and Other Laws (Amendment) Act 2019

- Aadhaar (Authentication) Regulations 2016
- Aadhaar (Data Security) Regulations 2016
- Aadhaar (Sharing of Information) Regulations 2016
- Any other Regulations or notices or Circulars issued by UIDAI from time to time.