Policy for Protecting Personal Data of Aadhaar Number Holders

By Appnit Technologies Private Limited

Document History

Version No	Date of Approval	Reviewed By	Approved By	Description of changes
1.0	28-04-2023	Nvneet Sharma	Board of Directors	Release

Abbreviations

Abbreviation	Description
ADV	Aadhaar Data Vault
ASA	Authentication Service Agency
AUA	Authentication User Agency
CERT-In	Indian Computer Emergency Response Team CIDR
	Central Identities Data Repository
e-KYC	Electronic Know Your Customer
e-Mail	Electronic Mail
HSM	Hardware Security Module
KUA	e-KYC User Agency
NDA	Non-Disclosure Agreement
OTP	One-Time Password
PID	Personal Identity Data
SMS	Short Message Service
STQC	Standardization Testing and Quality Certification
UIDAI	Unique Identification Authority of India
UID Token	Unique ID Token
VID	Virtual ID

Table of Contents

1. Terms and Definitions:

a) "***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

b) "***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

c) "***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

d) "***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

e) ***"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

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

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

g) "***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

h) "***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

i) "***Central Identities Data Repository***" (**CIDR**) means a centralized 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

j) "***Consent***" means the consent referred to in section 11 of PDP bill 2019

Reference: section 11 of PDP bill 2019 (given below)

(1) 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.

k) ***"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

l) "***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

m) "***e-KYC User Agency***" or "***KUA***" shall mean the 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

n) "***Global AUAs***" means the agencies which will have access to full e-KYC (with Aadhaar number) and the ability to store Aadhaar number within their system.

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

o) ***"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-11020/217/2018UIDAI (Auth-I), dated 10th January 2018

p) "***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

q) “***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

r) “***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

s) “***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

t) ***“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

u) ***“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

v) ***"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

w) “***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

x) *“**Requesting Entity***” means **Appnit Technologies Pvt. Ltd. ("Oxymoney”),** a company incorporated under the Companies Act, 1956/Companies Act, 2013, as amended, bearing CIN: U72900UP2014PTC063266 and having its registered office at Stellar OKAS

1425, Plot No.5, Sector 142, Noida, Gautam Buddha Nagar, Uttar Pradesh, Pin Code - 201305, India, that, shall submit 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

y) "***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

z) *"**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

aa) "***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

bb) "***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

2. Purpose

The purpose of this policy is to provide direction to the various stakeholders and responsible personnel within Appnit Technologies Pvt. Ltd. **("Oxymoney")** to protect the 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.

3. Personal Data collection

Oxymoney shall collect the personal data including Aadhaar number/Virtual ID, directly or indirectly through a third party, from the Aadhaar number holder for conducting authentication with UIDAI at the time of providing the services.

4. 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 PoI (proof of identity) and PoA (proof of address) to perform KYC (Know your customer) by OXYMONEY as per RBI (Reserve Bank of India) guidelines for the financial 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.

5. Notice / Disclosure of Information to Aadhaar number holder

a) 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 Appnit Technologies Pvt. Ltd., being the entity collecting and processing the personal data;

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

6. 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 Oxymoney shall maintain logs of disclosure of information and Aadhaar number holder's consent.

7. Processing of Personal data

a) 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;

b) Oxymoney 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.

c) For 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.

8. Retention of Personal Data

The authentication transaction logs shall be stored/archived for a period of ten years as per the regulations governing the entity, 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.

9. 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.

10. 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) 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;

c) 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;

d) e-KYC information shall be stored in encrypted form only. Such encryption shall match UIDAI encryption standards and follow the industry's best practice.

e) Oxymoney (as and when classified as Global AUA and KUA, in due course) 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; <*Applicable to global AUAs*>

f) 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;

g) Oxymoney shall use only Standardization Testing and Quality Certification (STQC) / UIDAI certified biometric devices for Aadhaar authentication (if biometric authentication is used);

h) 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;

i) In the event of an identity information breach, the organization 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 Grievance Officer's contact details;
- Measures taken to mitigate the identity information breach;

j) 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;

k) 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;

l) Best practices in data privacy and data protection based on International Standards shall be adopted;

m) 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.

n) 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.

o) Aadhaar numbers shall only be stored in Aadhaar Data vault as per the specifications provided by UIDAI.

11. 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) Oxymoney 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.

c) The Aadhaar number holder may, at any time, revoke consent given to OXYMONEY for storing his e-KYC data, and upon such revocation, OXYMONEY 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.

12. Aadhaar Number Holder Access Request

a) 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.

b) All requests from the Aadhaar number holder shall be formally recorded and responded to within a reasonable period.

c) Compliance with the relevant data protection / privacy law (s) shall be ensured.

13. Privacy by Design

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) Oxymoney, 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, the organization 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) 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.

14. Accountability Obligations

a) e-KYC shall be carried out using only biometric and/or OTP authentication modalities.

b) Appnit shall comply with all terms and conditions outlined in the Aadhaar Act 2016 and various circulars/ directions issued by the UIDAI.

c) Necessary Information security training shall be conducted for all personnel for Aadhaar related authentication services during induction.

d) Appnit will nominate a management point of contact and a technical point of contact for Aadhaar related activities and communication, if any, with the concerned authorities.

e) Appnit shall execute the relevant substantive documentation from its third-party incorporating confidentiality obligations for their personnel handling Aadhaar related data.

f) Access to Authentication infrastructure shall not be granted before signing the necessary substantive documentation and completion of BGV for the personnel.

15. Transfer of Identity information outside India is Prohibited

Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhaar Act and its Regulations.

16. 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 etc.

b) Reasonable measures shall be taken to inform the residents / customers / individuals about the Grievance Officer and its contact details;

c) 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;

d) 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 Grievance Officer and contact details;

e) If any issue is not resolved through consultation with the management of Appnit**,** Aadhaar number holders can seek redressal by way of mechanisms as specified in Section 33B of the Aadhaar Act, 2016.

17. Relevant Provisions of Aadhaar Act and Supreme Court Judgement

Following relevant 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

18. Contact Details

In case of any grievance / review of information, you may contact the coordinates provided below:

- Grievance Officer
  Contact details: grievance@oxymoney.com

Or write to us at:

- Grievance Officer
  Oxymoney C/O Appnit Technologies Private Limited,
  Unit-11-A, Stellar Okas 1425, 11th Floor,
  Plot Number 5, Sector 142, Noida
  Gautam Buddha Nagar, Uttar Pradesh-201305