SAMUNNATI FINANCE PRIVATE LIMITED	
POLICY	Privacy & Disclosure Policy
Reviewing Authority:	IT Strategy Committee
Approving Authority:	Board of Directors
Original Issue Date:	December 20, 2024
Version No:	1
Date of approval by Policy Approval Committee	December 20, 2024
Date of last review	May 19, 2026
Effective Date	December 20, 2024
Review Cycle:	Annually or as recommended by the Board of Directors

Privacy & Disclosure Policy

Samunnati Finance Private Limited ("the Company") recognizes the expectations of its customers with regard to privacy, confidentiality and security of their personal information that resides with the Company. Keeping personal information of customers secure and using it solely for activities related to the Company and preventing any misuse thereof is a top priority of the Company. The Company has adopted the privacy policy aimed at protecting the personal information entrusted and disclosed by the customers **["the Policy"]**. This policy governs the way in which the Company collects, uses, discloses, stores, secures and disposes of personal information and sensitive personal data or information.

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.

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.

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.

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.

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.

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

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.

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

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.

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

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.

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.

m) "***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.

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.

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.

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.*

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

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.

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.

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.

u) ***"Personnel"*** means all the employees, staff and other individuals employed/contracted by the requesting entities.

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, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment, or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction.

w) ***"Reference Key"*** means an additional key which is mapped with each Aadhaar number stored in the Aadhaar data vault.

x) ***"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.

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.

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.

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.

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 regulation.

Applicability

This Policy is applicable to personal information and sensitive personal data, or information collected by the Company or its affiliates directly from the customer or through the Company's online portals, mobile apps and electronic communications as also any information collected by the Company's server from the customer's browser.

Purpose of Collection and Use of Personal Information

The Company collects and uses the financial information and other personal information from its customers. This information is collected and used for specific business purposes or for other related purposes designated by the Company or for a lawful purpose to comply with the applicable laws and regulations. The Company shall not divulge any personal information collected from the customer, for cross selling or any other purpose.

The Company collects 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.

The authenticity of the personal information provided by the customer shall not be the responsibility of the Company.

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

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 long term or short-term loan to cater the financial needs for the purpose of carrying on Agri related activities

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

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

   i. The purpose for which personal data / identity information is being collected.

   ii. The information that shall be returned by UIDAI upon authentication.

   iii. 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.

   iv. The alternatives to submission of identity information (if applicable).

   v. 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.

   vi. The information that Virtual ID can be used in lieu of Aadhaar number at the time of Authentication.

   vii. The name and address of the Company 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 the Company shall maintain logs of the same.

Disclosure of Personal Information

The personal information collected by the Company shall not be disclosed to any other organization except:

1. where the disclosure has been agreed upon in a written contract or otherwise between the Company and the customer.
2. where the Company is required to disclose the personal information to a third party on a need-to-know basis, provided that in such case the Company shall inform such third party of the confidential nature of the personal information and shall keep the same standards of information/ data security as that of the Company.
3. Furnished pursuant to any directions of a governmental authority or court of law.

Obtaining Consent

a) 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 the Company shall maintain logs of disclosure of information and Aadhaar number holder's consent.

b) 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 the Company 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) The Company shall not use the Identity information including Aadhaar number or e-KYC for any other purposes than allowed under Master Direction on Know Your Customer Norms, Prevention of Money Laundering Act,2002, The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 and other applicable laws as modified from time to time <*Specific applicable law to be mentioned by the requesting entity*> 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

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.

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.

c) The Company 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.

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 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 entity 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) The Company 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.
g) The Company 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.
h) 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.

i) The Company 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;

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

   i. A description and the consequences of the breach.

   ii. A description of the number of Aadhaar number holders affected and the number of records affected.

   iii. The privacy officer's contact details.

   iv. Measures taken to mitigate the identity information breach.

k) 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.

l) 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.

m) Best practices in data privacy and data protection based on international Standards shall be adopted.

n) The response received from CIDR in the form of authentication transaction logs shall be stored with following details:

   i. 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.

   ii. Specified parameters received as authentication response.

   iii. The record of disclosure of information to the Aadhaar number holder at the time of authentication; and

   iv. Record of consent of the Aadhaar number holder for authentication but shall not, in any event, retain the PID information.

o) 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.

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

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) The Company 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.

c) The Aadhaar number holder may, at any time, revoke consent given to the Company for storing his e-KYC data, and upon such revocation, the Company 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 privacy officer who is responsible for monitoring of the identity information processing activities so that the processing is not in contravention of the law.

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 to the relevant data protection / privacy law (s) shall be ensured.

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) The Company 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) 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.

Governance and Accountability Obligations

a) A Privacy committee shall be established to provide strategic direction on Privacy matters.

b) 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.

c) The name of the Privacy Officer and contact details shall be made available to UIDAI and other external agencies through appropriate channel.

d) The Privacy Officer shall be responsible to assess privacy risks of processing Identity information / personal data and mitigate the risks.

e) The Privacy Officer shall be independent and shall be involved in all the issues relating to processing of identity information.

f) The Privacy Officer shall be an expert in data protection and privacy legislations, regulations, and best practices.

g) The Privacy Officer shall advise the top management on the privacy obligations.

h) The Privacy Officer shall advise on high-risk processing and the requirement of data privacy impact assessments.

i) 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.

j) The Privacy Officer shall be responsible for managing privacy incidents and responding to the same.

k) 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.

l) Privacy officer shall ensure that the Authentication operations, systems and applications are audited by CERT-IN (Indian Computer Emergency Response Team), Standardization Testing and Quality Certification (STQC) empaneled auditors or any other UIDAI recognized body at least on an annual basis;

m) Privacy officer shall conduct internal audits (through internal audit team) on a quarterly basis and monitor compliance through these audits against Aadhaar Act 2016.

n) 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.

o) 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.

p) 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.

q) 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.

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.

Grievance Redressal Mechanism

a) Aadhaar number holders with grievances about the processing can contact the organization's Privacy 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 Privacy Officer and its contact details.

c) The contact details of Privacy Officer and the format for filing the complaint shall be displayed on the organizations' 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 Privacy officer and contact details.

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

Responsibility for implementation and enforcement of the policy

Samunnati shall identify and assign responsibilities to ensure implementation and enforcement of the Policy.

Reasonable Security Practices and Procedures

The security of personal information is priority and will be protected by maintaining physical, electronic, and procedural safeguards that meet applicable laws. The Company shall take reasonable steps and measures to protect the security of the customer's personal information from misuse and loss, un-authorized access, modification or disclosure. The Company will maintain its security systems to ensure that the personal information of the customer is appropriately protected and follows the extant standard encryption norms followed for the transmission of information. The Company will ensure that its employees and affiliates respect the confidentiality of any personal information held by the Company.

Exclusions

Notwithstanding anything mentioned in the Policy, the Policy shall exclude information that is needed to be shared with others due to extant regulations e.g. credit bureaus, CKYC registry, ROC and RBI and also where the Company is legally bound to disclose information including but not limited to FIU, Enforcement Directorate, IT department or as required by a Court of Law.

Contact Information

In order to address any discrepancies or grievances related to the personal information residing with the Company, the customers may contact the Grievance Officer of the Company, who will act as the grievance officer under this policy, at customervoice@samunnati.com

Notice of change

Amendments to this Policy shall be carried out subject to approval of the Board of Directors.

Cookie policy

The Company's digital platforms use various third-party analytical tools. These tools use cookies which are downloaded to your device when you visit a website in order to provide a personalized browsing experience. Cookies are used for lots of tasks like remembering your preferences & settings, provide personalized browsing experience and analyze site operations. These cookies collect information about how users use a website, for instance, how often visited pages. All information collected by third party cookies is aggregated and anonymous. By using our website user/s agree that these types of cookies can be placed on his/her device. User/s is free to disable/delete these cookies by changing his/her device / browser settings. The Company is not responsible for cookies placed in the device of user/s by any other website and information collected thereto.

Effective Date

The policy would come into effect from the date of review and approval by the Board of Directors.