Personal Data Collection

ACAB 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 Aadhaar related services.

Specific purpose for collection of Personal data

a) The Identity information including Aadhaar number / Virtual ID shall be collected for the purpose of authentication of Aadhaar number holder to provide Aadhaar enabled payment service & e-KYC service.

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. Name and address of ACAB which is 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 ACAB shall maintain logs of the same.

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

ACAB 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 ACAB 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) ACAB shall not use the Identity information including Aadhaar number or e-KYC for any purposes other than the ones declared to UIDAI or permitted by UIDAI 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) ACAB 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;

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

j) 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;

k) In the event of an identity information breach, the organisation 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;

l) 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;

m) 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;

n) Best practices in data privacy and data protection based on international Standards shall be adopted;

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

p) 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.

q) 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 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.

b) ACAB 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 ACAB for storing his e-KYC data, and upon such revocation, ACAB 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;