Government of NCT of Delhi
DEPARTMENT OF INFORMATION TECHNOLOGY
9th Level, B-Wing, Delhi Secretariat
IP Estate, New Delhi-110002

F. No. E-13/2/2022-Development/6266-6345 Dated: 29/07/26

Circular

Subj.: Regarding implementation of Aadhaar Data Vault (ADV).

Please refer to the UIDAI Circular No. 11020/205/2017-UIDAI(Auh-I) dated 25.01.2017(copy enclosed) wherein it has been informed that Aadhaar Number is being used as primary ID of the residents by various user organizations like Banks, Telecoms, Government departments, Income Tax department, Private Sectors, etc. To avail the different benefits/services, Aadhaar Number Holder has to share the Aadhaar Number to various entities and the entities store the Aadhaar Numbers as reference key to deliver their services/benefits.

2. In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all the entities that are collecting and storing the Aadhaar number for specific purposes shall start using "Aadhaar Data Valut" (ADV) i.e on a separate secure database/vault/ system.

3. In compliance with UIDAI guidelines, IT Department, GNCTD in coordination with Delhi State NIC has implemented ADV for e-district portal to ensure secure storage of Aadhaar data stored in database.

4. Departments of GNCTD who are storing Aadhaar Numbers in their database are also requested to implement Aadhaar Data Vault services either on its own through any authorized agency or through ADV of Department of Information Technology, GNCTD provided by CDAC. The IT Department has signed the Memorandum of Understanding (MoU) with CDAC for providing the Aadhaar Data Vault Services.

5. In order to utilise the Aadhaar Data Vault of Department of IT, GNCTD following is required to be adhered to by the user Departments: -

a. The Department will sign a formal agreement (**Annexure-I**) with DIT, GNCTD. Any lapses by any participating entity during the retrieval or storage of Aadhaar numbers in ADV shall be the responsibility of the user Department. Additionally, data will be shared among all departments through a common repository maintained under the name of DIT, Delhi GNCTD.

b. As the data will be shared among all departments through a common repository maintained under the name of DIT, Delhi GNCTD the option to delete any Aadhaar number stored in ADV shall not be given to any other Department of GNCTD.

c. The financial implication for providing the ADV facility will be borne by the IT Department, GNCTD.

6. For the departmental services hosted on e-district portal, there is no need of ADV from departmental side as the same has been implemented by IT Department, GNCTD.

7. The departments of GNCTD, who wish to utilise the facility of ADV through IT Department may contact IT Department, GNCTD along-with department on boarding form (**Annexure-II**), details of approximate number of transactions (Quarterly) expected and total number of Aadhaar to be stored in ADV.

This issues with the approval of the Competent Authority.

Enclosures: As above.

(K. Murugan)
Joint Director (IT)

F. No. E-13/2/2022-Development/6266-6345 Dated: 28/07/26

Encl.: A/A

To,

All Addl. Chief Secretaries/Pr. Secretaries/Secretaries/HODs, Government of NCT of Delhi

Copy for information to:

1. Secretary to Hon'ble Lieutenant Governor, GNCTD
2. Secretary to Hon'ble Chief Minister, GNCTD
3. Secretaries to all Hon'ble Ministers, GNCTD
4. Staff Officer to Chief Secretary, GNCTD
5. PA to Secretary (IT), GNCTD
6. PS to Special Secretary (IT), GNCTD
7. Guard File

(K. Murugan)
Joint Director (IT)

सं .के-11020/205/2017- यूआईडीएआई (ऑथ-I)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथंटीकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001
दिनांक: 25.07.2017

Circular

Aadhaar Number is being used as primary ID of the residents by various user organizations like Banks, Telecoms, Government departments, Income Tax department, Private Sectors, etc. To avail the different benefits/services, Aadhaar Number Holder has to share the Aadhaar Number to various entities and the entities store the Aadhaar Numbers as reference key to deliver their services/benefits.

In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all AUAs/KUAs/Sub-AUAs and other entities that are collecting and storing the Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference Keys mapped to Aadhaar numbers through tokenization in all systems.

The course of action to implement the process by all AUAs/KUAs/Sub-AUAs and other entities is hereby outlined as below:

(a) All entities are directed to mandatorily store Aadhaar Numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where the Aadhaar Number and any connected Aadhaar data will be stored.

(b) Entities are allowed to store any relevant demographic data and/or photo of the Aadhaar Number Holder in other systems (such as customer database) as long as Aadhaar Number is not stored in those systems.

(c) Each Aadhaar number is to be referred by an additional key called as Reference Key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

(d) All business use-cases of entities shall use this Reference Key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than Aadhaar Data Vault.

(e) Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

25/7/17

(f) The Aadhaar number and any connected data maintained on the Aadhaar Data Vault shall always be kept encrypted and access to it strictly controlled only for authorized systems. Keys for encryption are to be stored in HSM devices only.

(g) Aadhaar numbers along with connected data if any (such as eKYC XML containing Aadhaar numbers and demographic data) shall only be stored in a single logical instance of Aadhaar Data Vault with corresponding reference key. Appropriate HA/DR provisions may be made for the vault with same level of security.

(h) The Aadhaar Data Vault containing Aadhaar number/data and the referencing system must be kept in a highly restricted network zone that is isolated from any untrusted zone and other internal network zones.

(i) Only trusted communications must be permitted in and out of the vault. This should ideally be done via API/Micro-service dedicated to get the mapping and controlling access to the API/Micro-service at application level. Any authorized users needing to access this mapping must go via applications allowing them to view/access this data with appropriate user authentication and logging.

(j) The Aadhaar Data Vault must implement strong access controls, authentication measures, monitoring and logging of access and raising necessary alerts for unusual and/or unauthorized attempts to access.

(k) The Aadhaar Data Vault should support mechanisms for secure deletion/updation of Aadhaar number and corresponding data if any as required by the data retention policy of the entities.

(l) The chosen Reference Key generation method is to ensure that the recovery of the original Aadhaar number must not be computationally feasible knowing only the reference key or number of reference keys. It is suggested that a UUID (Universally Unique Identifier represented via hex string) scheme be used to create such reference key so that from such reference key, Aadhaar number can neither can be guessed nor reverse engineered.

Therefore in exercise of the provisions of Regulation 14(n) of the Aadhaar (Authentication) Regulations, 2016 and Regulations 5 and 6 of Aadhaar (Sharing of Information) Regulations, 2016, any non-compliance shall be dealt under Section 42 of the Aadhaar Act, 2016 and shall also attract financial disincentives as per the schedule of the AUA/KUA agreement.

Yashwant 21/7/17

(Yashwant Kumar
Assistant Director General
दूरभाष : 011-23462606

To

1. All AUAs/KUAs and ASAs.
2. UIDAI Tech Center, Bengaluru

Annexure-I

This **Provisioning of Aadhaar Data Vault Service Agreement** ("**Agreement**") is made as of this

____day of_____("**Effective Date**"), at_____,

By and Between:

1. **Department of Information Technology, Govt of NCT of Delhi** having its registered office at '**B**' **Wing 9th level, Delhi Secretariat, New Delhi** (hereinafter referred to as '**DIT Delhi**', which expression shall unless repugnant to the content or meaning thereof, include its successors and permitted assigns, as the case may be);

AND

2. **Department Name**

(hereinafter collectively referred to as "**Department Entities**" or individually as **"Department Entity"**) OF THE OTHER PART.

Each of the parties mentioned above is collectively referred to as the '**Parties**' and individually as a'**Party**' and has their registered offices as follows:

Mention each party address and name (Applicable for Multiparty)

It is hereby expressly agreed and acknowledged by the Parties that the concerned Department Entity is availing the Aadhaar Data Vault (ADV) services through the **Department of Information Technology, Govt of NCT of Delhi** (hereinafter referred to as "DIT Delhi"), and accordingly, such Department Entity shall be governed by, and hereby expressly agree to be bound by and comply with, all applicable terms, conditions, obligations and provisions as set forth in the existing Agreement/Memorandum of Understanding executed between DIT Delhi and C-DAC, which is hereby incorporated by reference into this Agreement, as may be amended from time to time; it is further clarified that the Department Entity shall not have any independent or additional rights, entitlements, or claims against C-DAC; DIT Delhi shall act as the nodal and coordinating authority for the provisioning, administration, and oversight of ADV services for the Department Entity, and all communications, requests, and obligations pertaining to the services shall be routed through or in coordination with DIT Delhi unless otherwise expressly agreed in writing, and this provision shall be read as an integral part of the present Agreement, with the terms of the Agreement between DIT Delhi and C-DAC prevailing in case of any inconsistency.

Annexure-C

Department and Application Registration form ☐ Staging ☐ Production

Table 1. Department Registration Form

Department Name	
Address	
Contact Person	
Designation	
Email	
Mobile	
Phone	
City	
State	
Pin code	
Category	Government / PSU / Private

Table 2. Application Registration Form

Application Name	
Description	
Contact Person	
Email	
API access required for	☐Store UID ☐Get UID ☐Get Reference Number ☐Activate ☐Deactivate ☐Delete ☐Userschemes
Same reference number required across all	○ Yes ○ No

applications registered under the department	
The reference number to be returned or error during stored UID API call, in case of already stored Aadhaar Number	○ Return Error ○ Return already generated reference number
Algorithm used for the encryption and decryption of data for all applications	AES-256
HSM Key allotted to the department will be used to encrypt and decrypt the data for all applications	Yes
Application Category	○ Same as Department ○ Government/ PSU /Private (Strike which is not applicable.)
Public IP (s) of the Department for which access to be provided	

Signature and Stamp of the Authorized Person

Note: Fill separate application registration form for multiple applications that need to be registered against the department.

The completion of IP Whitelisting for the Aadhaar Data Vault Service in the Staging Environment may take up to 03 working days and for the Production Environment it may take around 07 working days as it involves the establishment of necessary policies and approvals.
