ERGO

KHAITAN & CO ADVOCATES SINCE 1911

Vaulting to safety:

UIDAI issues clarifications on applicability of Aadhaar Data Vault requirements

10 December 2025

On 3 November 2025, the Unique Identification Authority of India (UIDAI) updated its 'Frequently Asked Questions (FAQs) on Aadhaar Data Vault (ADV) / Hardware Security Module (HSM)'[1] (2025 FAQs), based on its revised ADV Circular[2] dated 18 July 2025 (2025 Circular). The 2025 Circular and 2025 FAQs have provided important clarifications on the applicability and scope of Aadhaar Data Vault (ADV) requirements pertaining to storage of Aadhaar data, and related security requirements for setting up and maintenance of ADVs.

1. Background

The Aadhaar Unique Identification scheme, under which unique 12-digit numbers were assigned to each Indian citizen for availing government benefits and services received its statutory backing with the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act 2016 (Aadhaar Act). The constitutionality of the Aadhaar scheme vis-à-vis the right to privacy was upheld by the Supreme Court of India in 2018[3], albeit with certain measures required for collection and storage Aadhaar related information (the judgment has been covered in detail in our ERGO Update here). These measures included security measures, data minimisation and allowing private entities such as banks, telecom service providers, etc. to collect Aadhaar numbers only on a voluntary basis by obtaining explicit and informed consent of users.

The UIDAI has also laid down the privacy requirements related to authentication and verification of Aadhaar by requesting entities (REs)[4] under the Aadhaar (Authentication) Regulations 2016 and the Aadhaar (Authentication and Offline Verification) Regulations 2021 (Aadhaar Regulations). REs include Authentication User Agencies (AUAs) and e-KYC User Agencies (KUAs) and entities availing these facilities through other AUAs / KUAs (Sub-AUAs and Sub-KUAs respectively). Additionally, the UIDAI has issued several circulars stipulating security measures to be undertaken in the process of storing Aadhaar numbers.

2. Circulars governing Aadhaar Data Vault

(i) **Definition of ADV**:

An ADV is defined by UIDAI as a centralised storage for all the Aadhaar numbers collected by the RE for specific purposes under Aadhaar Act and Aadhaar (Authentication) Regulations 2016. It is a secure system inside the respective RE's infrastructure accessible only to authorised personnels on a need-to-know basis.

[1] 'Frequently Asked Questions (FAQs) on Aadhaar Data Vault (ADV) / Hardware Security Module (HSM)' issued by Unique Identification Authority of India dated 3 November 2025, https://uidai.gov.in/images/FAQs_Aadhaar_Data_Vault_03112025_v10.pdf.

[2] Circular No. 8 of 2025 (F. No. HQ-13031/1/2022-AUTH-I HQ) issued by Unique Identification Authority of India dated 18 July 2025 < https://uidai.gov.in/images/Circular_8_of_2025-Revised_guidelines_for_ADV_HSM.pdf.

[3] K S Puttaswamy and Another vs Union of India, 2017 (10) SCC 1.

[4] Agencies or persons that submit the Aadhaar number / demographic information / biometric information of an individual for authentication

(ii) **Guidance on storage of ADV**:

The first circular on ADV was issued by the UIDAI on 25 July 2017[5] (2017 Circular) containing a detailed course of action by AUAs / KUAs / Sub-AUAs and other entities while storing Aadhaar numbers and connected data, to prevent misuse and unauthorised access. This includes:

(a) Storing of Aadhaar numbers and any connected data (*e.g.* e-KYC Extensible Markup Language (XML) containing Aadhaar number and data) only on a separate secure database / vault designated as ADV;

(b) Encrypting ADV, storing of encryption keys in HSM devices not shared with any other entity, and maintaining ADV in a highly restricted network zone;

(c) Referencing of each Aadhaar number with an additional key which does not computationally permit reverse engineering / guessing of Aadhaar number (**Reference Key**) and maintaining the mapping of Aadhaar numbers and Reference Keys on the ADV;

(d) Using only the Reference Keys in all business use-cases instead of actual Aadhaar numbers; and

(e) Implementing strong access controls, monitoring and logging of access to ADV.

(iii) **Applicability of ADV requirements**:

The UIDAI in its frequently asked questions on the 2017 Circular[6] (2017 FAQs) clarified that the above-mentioned requirements in relation to ADVs are applicable to '*AUAs / KUAs / Sub-AUAs and other entities*' involved in storage of Aadhaar numbers (including masked Aadhaar numbers). The implication of this clarification was that organisations which had not availed UIDAI authentication or verification facilities but had stored Aadhaar numbers (including masked Aadhaar number) of its employees in a digital form would also have to comply with the ADV requirements. Subsequent FAQs released in 2022 omitted the aforesaid applicability requirement and remained silent in terms of specifying the exact nature of entities to which ADV requirements would be applicable.

(iv) **Clarity on Offline Verification Seeking Entities**:

Subsequently in 2024, the UIDAI in its FAQs on role of Offline Verification Seeking Entities (OVSEs), clarified that OVSEs which were collecting Aadhaar information for offline verification purpose without availing authentication facility from UIDAI need not comply with the ADV requirements.[7] These varied circulars and clarifications issued by the UIDAI created confusion among entities collecting Aadhaar information or entities undertaking Aadhaar authentication as to the exact compliance requirements applicable to them.

3. 2025 Circular and FAQs

Through the 2025 Circular and 2025 FAQs, two important clarifications have been made, clarifying the scope and applicability of ADV requirements and resolving the confusion that earlier prevailed.

(i) **Applicability of ADV requirements**:

The 2025 Circular and 2025 FAQs now clarify that ADV requirements only apply to REs and not to other entities like OVSEs or entities collecting Aadhaar information of employees for internal purposes (without referring the same to UIDAI for verification). Accordingly, it has also been clarified that the data stored in ADV must flow from the UIDAI (*i.e.* post-authentication) and REs cannot directly store data from the input received from users (*i.e.*, Aadhaar number holders) for authentication.

[5] Circular No. 11020-205/2017 issued by Unique Identification Authority of India dated 25 July 2017, available at https://uidai.gov.in/images/resource/Circular_Reference_Key_02082017.pdf.

[6] Question 4 of 'Frequently Asked Questions (FAQs) – Aadhaar Data Vault / Reference Keys Ref: UIDAI Circular' issued by Unique Identification Authority of India dated 25 June 2017 <https://uidai.gov.in/images/resource/FAQs_Aadhaar_Data_Vault_v1_0_13122017.pdf>.

[7] Question 8 of 'Aadhaar: Frequently Asked Questions (FAQs) on Offline verification process of Aadhaar and role of Offline verification seeking entities (OVSEs) issued by Unique Identification Authority of India dated 11 July 2024 <https://uidai.gov.in/images/FAQ_OVSE.pdf>.

Further, the ADV requirements have been made more stringent. While earlier, any isolated system / storage environment could be used by an entity as its ADV, the 2025 Circular specifies that only three types of environments may be used for hosting the ADV of an RE: (i) within the secure premises of the RE, (ii) on a cloud based on the Government Community Cloud (GCC), empanelled by the Ministry of Electronics & Information Technology (MeitY), or (iii) ADV-as-a-service provided by an entity.

Further, Sub-AUAs/Sub-KUAs may implement their own ADV or use their respective AUA's / KUA's ADV as-a-service subject to ensuring logical segregation. In addition, Sub-AUAs/Sub-KUAs are fully responsible for ensuring compliance with respect to the Aadhaar Act and associated regulations.

Other data security requirements have also been prescribed by the 2025 Circular, such as HSM, encryption standards of AES-256 or above and compliance of the GCC / ADV provider with UIDAI security standards. Sub-AUAs / Sub-KUAs have been permitted to use their respective AUA's / KUA's HSM, provided that the HSM configuration must ensure logical isolation / segregation for each RE and dedicated crypto keys for each RE. AUAs and KUAs cannot access data in the ADV of their Sub-AUAs / Sub-KUAs.

(ii) **<u>Scope of 'connected data'</u>**:

Earlier, the scope of data to be stored in ADV was unclear, only having been specified as including Aadhaar number and "any connected data (*e.g.* e-KYC XML)". The 2025 Circular and 2025 FAQs have clarified that the data to be stored in ADV include Aadhaar number, UID token, e-KYC XML containing Aadhaar number, Aadhaar PDF received from e-KYC response and Aadhaar-related demographic data (Aadhaar number along with name, date of birth, gender, address, photo, email address and mobile number).

However, demographic details have also been allowed to be stored locally (*i.e.* outside the ADV) if Aadhaar number and UID Token are not stored / mapped with it, taking reasonable security safeguards like encryption, obfuscation or masking of Aadhaar-independent demographic data. Likewise, the UID Token without demographic details can also be stored locally while ensuring reasonable security safeguards. The requirement to ensure 'reasonable security safeguards' is in line with the compliances relating to personal data under the Digital Personal Data Protection (DPDP) Act, 2023 and the recently-notified DPDP Rules, 2025.

4. Conclusion

Through the 2025 Circular and 2025 FAQs, the UIDAI has brought in much-needed clarity for entities collecting Aadhaar information. REs should re-evaluate their ADV data storage policies and procedures, infrastructure and security measures.

- *Smita Jha (Partner); Pritish Mishra (Principal Associate) and Ananya Giri Upadhya (Associate)*

About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**

This document has been created for informational purposes only. Neither Khaitan & Co nor any of its partners, associates or allied professionals shall be liable for any interpretation or accuracy of the information contained herein, including any errors or incompleteness. This document is intended for non-commercial use and for the general consumption of the reader, and should not be considered as legal advice or legal opinion of any form and may not be relied upon by any person for such purpose. It may not be quoted or referred to in any public document, or shown to, or filed with any government authority, agency or other official body.