COLLECTION AND STORAGE OF AADHAAR DATA | THINGS TO LOOK OUT FOR

1. INTRODUCTION

The Unique Identification Authority of India ("**UIDAI**") was set up under the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("**Aadhaar Act**") to issue the 12-digit unique identity number ("**Aadhaar Number**") (indicated on a card and hereinafter referred to as the "**Aadhaar Card**") to all residents in India.[1] The UIDAI has already issued Aadhaar Numbers to over 1.3 billion residents of India.[2] Introduced with the objectives of (i) eliminating the risk of fake identities and (ii) providing cost effective means of verification and authentication of the identity of an individual, Aadhaar Cards have found widespread acceptability in India. Despite the Supreme Court of India ruling that the furnishing of Aadhaar Cards cannot be mandated unless required by a law in force,[3] Aadhaar Cards continue to be one of the most frequently used and accepted identity and address proof documents

Unlike most other identity and address proof documents, there are regulatory requirements on collection, storage and processing of Aadhaar Numbers. The Aadhaar Act and corresponding regulations prescribe in granular detail the requirements on collection, use and storage of Aadhaar Numbers and Aadhaar Cards.

2. WHO CAN COLLECT AADHAAR DATA?

As per the Aadhaar Act, the following categories of persons are permitted to collect Aadhaar information:

a. A requesting entity[4] for conducting Aadhaar authentication;[5] and

b. Any person for conducting know your customer verification, or for any other lawful purpose.

3. REGULATIONS FOR COLLECTION, USE AND PROCESSING OF AADHAAR INFORMATION

The Aadhaar (Sharing of Information) Regulations, 2016 ("**Sharing of Information Regulations**") prescribe the manner for the collection, use, circulation, transfer, or publication of the Aadhaar Number or any document containing the Aadhaar Number (such as a scanned image of the Aadhaar Card) along with the liability for any contravention. As per the Sharing of Information Regulations, a person can collect Aadhaar Number from the data subject ("**Holder**") by complying with the following broad principles:

---

[1] "Resident" has been defined under Section 2(v) of the Aadhaar Act as 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.

[2] About UIDAI, available at, https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html

[3] Justice K.S. Puttaswamy (Retd) v. Union of India, Writ Petition (Civil) No. 494 of 2012.

[4] "Requesting Entity" has been defined under Section 2(u) of the Aadhaar Act as an agency or person that submits the Aadhaar Number, and demographic information or biometric information, of an individual to the Central Identities Data Repository ("**CIDR**") for authentication.

[5] "Authentication" has been defined under Section 2(c) of the Aadhaar Act as the process by which the Aadhaar Number along with demographic information or biometric information of an individual is submitted to the CIDR for its verification. The CIDR verifies the correctness of the information submitted and on the basis of information already available in its systems.

a. Consent: Obtaining of prior consent of the Holder;[6]

b. Purpose Limitation: Prohibiting use of the Aadhaar Number for any purpose other than that specified to the Holder at the time of collection;

c. Alternatives: Providing alternate options to the submission of the Aadhaar Number, if any, provided that the submission of Aadhaar Number is not mandated by law.[7]

Once collected, the Aadhaar Number must not be published, displayed or posted publicly and the entity collecting the Aadhaar Number must ensure the security and confidentiality of the Aadhaar Number and of any record or database containing the Aadhaar Number. Transmission of Aadhaar Numbers must be done securely over the internet only if the Aadhaar Number is encrypted. Further, such entity must ensure that the Aadhaar Numbers are not retained for longer than is required for the purpose specified at the time of its collection. It is to be noted that provisions of the Sharing of Information Regulations pertaining to transmission, display and retention refer to only the Aadhaar Number and do not clarify if they are applicable to any document containing the Aadhaar Number, resulting in some regulatory ambiguity.

4 HOW TO STORE AADHAAR NUMBERS?

All persons storing Aadhaar Numbers[8] must store them in a separate and secure database ("**Aadhaar Data Vault**")[9] where the Aadhaar Numbers are masked by way of reference keys. The Aadhaar Data Vault is a centralised storage for all Aadhaar Numbers and is a secure system within the infrastructure of the person collecting the Aadhaar Numbers. In addition to keeping the Aadhaar Numbers secure, the Aadhaar Data Vault also seeks to reduce the footprint of Aadhaar Numbers within the organization's systems and reduces the risk of unauthorised access.

The decision on the technology to be used for the Aadhaar Data Vault lies with the respective person collecting the Aadhaar data from the Holders. While the UIDAI has prescribed certain technology specifications that may be adopted to ensure the security of the Aadhaar Data Vault, it has generally allowed adoption of the industry best practices to secure the Aadhaar Numbers in the Aadhaar Data Vault.

5 HOW TO STORE SCANNED OR HARD COPIES OF AADHAAR CARDS?

An entity which is storing the scanned and physical copies of Aadhaar Cards and is not storing the Aadhaar Numbers separately, does not need to comply with the Aadhaar Data Vault requirement. As per FAQs published by the UIDAI,[10]scanned copies of Aadhaar Cards must be stored in an encrypted form.

On the other hand, the UIDAI does not lay down the manner of collection of physical copies of Aadhaar Cards, but mandates that they must be stored in a secure manner.

Separately, it must be noted that scanned copies of Aadhaar Cards which contain the photograph of the Holder may be regarded as biometric information and consequently be considered sensitive personal data

[6] See Section 8 of the Aadhaar Act, along with Regulation 3 and Regulation 5 of the Sharing of Information Regulations.
[7] In the event the submission of Aadhaar Number or proof of Aadhaar is mandated by law for a particular purpose, then the Holder must be informed of the legal provision mandating it by the person collecting the Aadhaar Number or the document containing the Aadhaar Number.
[8] An offline verification seeking entity cannot store the Aadhaar Number of an individual.
[9] Circular No 11020/205/2017 issued by UIDAI available at https://uidai.gov.in/images/resource/Circular_Reference_Key_02082017.pdf.
[10] Aadhaar Data Vault FAQs published by the UIDAI, available at https://uidai.gov.in/images/resource/FAQs_Aadhaar_Data_Vault_v1_0_13122017.pdf

or information ("**SPDI**").[11] As a result, the storage, processing or disclosure of scanned copies or images of Aadhaar Cards may need to comply with the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("**SPDI Rules**"), in addition to the Aadhaar Act and the Sharing of Information Regulations.

A few of the key compliances under the SPDI Rules include publication of the privacy policy by the body corporate[12] collecting SPDI; [13] appointment of a grievance officer whose name and contact details must be published on the website of the body corporate; [14] and restrictions on disclosures along with transfer of SPDI. The SPDI Rules also mandate the adoption of reasonable security practices and procedures for storage of SPDI.[15] Such reasonable security practices and procedures maintained by the body corporate must be audited at least once a year or as and when the body corporate undertakes a significant upgrade of its computer resources,[16] by an independent auditor approved by the Government of India.

Non-compliance with the SPDI Rules may result in imprisonment along with fines and payment of compensation to the affected party.[17]

6 CONCLUSION

Although the UIDAI has been clear in its objective of allowing the collection and storage of Aadhaar Numbers by persons for lawful purposes, with the view of preventing misuse of such information, the Comptroller and the Auditor General ("**CAG**") in its first ever performance audit of the UIDAI has flagged a range of concerns and flaws with the functioning of the UIDAI. It has observed that UIDAI generated Aadhaar Numbers with incomplete information, which, along with the lack of proper documentation or poor-quality biometrics, have resulted in multiple or duplicate Aadhaar Cards being issued to the same person. It has also criticised the UIDAI for "deficient data management" considering instances where data of Holders have not been matched with their Aadhaar Numbers even after 10 years. In light of the concerns flagged above, the UIDAI must adopt remedial measures as suggested by the CAG at the earliest such that its objective of keeping Aadhaar Numbers secure along with preventing the misuse of Aadhaar Numbers can be fulfilled and the rules governing the protection of Aadhaar Numbers and document containing the Aadhaar Numbers are upheld in their letter and spirit.

Authors: Shreya Suri | Naqeeb Ahmed Kazia | Abhijit Chakrabarti

Practice Areas: Technology, Media & Telecommunications, Governance & Regulatory

Date: May 17, 2022

DISCLAIMER

[11] Section 30 of the Aadhaar Act, read with Section 2(g) of the Aadhaar Act.
[12] "Body corporate" has been defined under Rule 2(c) of the SPDI Rules read with Section 43A of the Information Technology Act, 2000 as "any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities."
[13] Rule 4 of the SPDI Rules.
[14] Rule 5 of the SPDI Rules.
[15] Rule 8 of the SPDI Rules. One such standard prescribed under the SPDI Rules is the international standard IS/ISO/IEC 27001.
[16] Ibid.
[17] Reference can be drawn to Section 43A and Section 72A of the Information Technology Act, 2000.