HQ-15035/4/2021/AU-HQ
Unique Identification Authority of India
(Aadhaar Usage Division)

UIDAI HQs,
Bangla Sahib Road, Behind Kali Mandir,
Gole Market, New Delhi. 110001

Dated: 31 October, 2022

CIRCULAR

Subject: Usage of Aadhaar - Dos & Don'ts for Requesting Entities- *Regarding*

A Requesting Entity (RE) is responsible for submitting the resident's Aadhaar number and demographic/ biometric/ OTP information, to the Central Identities Data Repository (CIDR), for the purpose of authentication.

2. An RE is engaged in providing Aadhaar authentication Services to an Aadhaar number holder, as facilitated by the Authentication Service Agency (ASA). The RE may be a government / private legal entity registered in India, which is authorized to use Aadhaar authentication services of UIDAI and sends authentication requests to enable its services / business functions. [Ref. Section '2-Definitions', Aadhaar (Authentication and Offline Verification) Regulations]

3. **Following are the Dos and Don'ts to be followed by the REs:**

DOs

i. Be courteous to residents. Assure the resident about the security & confidentiality of their Aadhaar number being used for authentication.

ii. Ensure that the resident clearly understands the type of data being collected and the purpose of Aadhaar authentication. Obtain resident's informed consent either on paper or electronically, prior to carrying out authentication.

iii. Store Aadhaar number only if you are authorized to do so and in the manner as prescribed by UIDAI i.e. within a secure Aadhaar Data Vault.

iv. Ensure that Aadhaar data collected is not shared with any entity except in accordance with the Aadhaar Act and/or regulations thereof.

v. Retain the logs of authentication transactions (including that of consents taken) only for the period as prescribed under Aadhaar (Authentication and Offline Verification) Regulations. Purging of such logs upon expiry of the period shall also be in accordance to the Aadhaar Act or regulations thereof.

vi. Ensure proper hygiene of the authentication devices being used so that there are minimal authentication failures

vii. Ensure regular training of operators/staff carrying out Aadhaar authentication on the best practices and safeguards involved in doing so.

viii. Immediately report any suspicious activity around authentication to UIDAI namely, suspected impersonation by resident, likely compromise of authentication keys of RE, likely fraud by authentication operator(s) etc.

ix. Cooperate with UIDAI and/or agencies deputed by UIDAI for the purpose of any security/ process audit as required by the Aadhaar Act/ Regulations or any other directions in this regard from UIDAI. Ensure timely closure of audit observations/non-compliances, if any.

x. Provide effective grievance handling mechanism to the resident via multiple channels like website, call center, mobile app, SMS, physical center, etc.

xi. Fulfill all your statutory obligations under the Aadhaar Act, 2016 including Penalties for contraventions (Section 29 and Chapter VIA of Aadhaar Act).

DON'Ts

i. Do not aid or abet any unlawful action of any resident/authentication operator/ other entity that is in contravention of the laws / regulations and prescribed processes & directions.

ii. Do not share your authentication keys/ certificates with any other entity.

iii. Do not share unique license keys/ code as provided by UIDAI with any other entity.

iv. Do not store photocopies of Aadhaar letters and/or other physical/electronic forms of Aadhaar, if used for collecting Aadhaar, without first masking / redacting the first 8 digits of the Aadhaar number displayed on those documents.

v. Do not store/share/publish the biometric information collected from the Aadhaar number holder for authentication.

vi. Do not act in contravention of the Aadhaar Act, 2016 and regulations thereof.

(Kuldeep Singh)
Asstt. Director (AU)
Tel: 2347 8511