The Aadhaar (Authentication) Regulations, 2016

CONTENTS

CHAPTER I
PRELIMINARY

Regulations		*Pages*
1.	Short title and commencement	80
2.	Definitions	80

CHAPTER II
AADHAAR AUTHENTICATION FRAMEWORK

3.	Types of Authentication	81
4.	Modes of Authentication	82
5.	Information to the Aadhaar number holder	82
6.	Consent of the Aadhaar number holder	83
7.	Capturing of biometric information by requesting entity	83
8.	Devices, client applications, etc. used in authentication	83
9.	Process of sending authentication requests	83
10.	Notification of authentication to Aadhaar number holder	84
11.	Biometric locking	84

CHAPTER III
APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES

12.	Appointment of Requesting Entities and Authentication Service Agencies	84
13.	Procedure where application for appointment is not approved	85
14.	Roles and responsibilities of requesting entities	85
15.	Use of Yes/No authentication facility	87
16.	Use of e-KYC authentication facility	87
17.	Obligations relating to use of identity information by requesting entity	88
18.	Maintenance of logs by requesting entity	88

Regulations *Pages*

19. Roles, responsibilities and code of conduct of Authentication Service Agencies 89
20. Maintenance of logs by Authentication Service Agencies 91
21. Audit of requesting entities and Authentication Service Agencies . 91
22. Data Security 92
23. Surrender of the access to authentication facility by requesting entity or Authentication Service Agency 92
24. Agencies appointed before commencement of these regulations ... 93
25. Liability and action in case of default 93

CHAPTER IV
AUTHENTICATION TRANSACTION DATA AND AUTHENTICATION RECORDS

26. Storage and Maintenance of Authentication Transaction Data 94
27. Duration of storage 94
28. Access by Aadhaar number holder 95

CHAPTER V
MISCELLANEOUS

29. Savings 95
30. Power to issue clarifications, guidelines and removal of difficulties 95

SCHEDULE A 96
SCHEDULE B 98
NOTIFICATION 99

The Aadhaar (Authentication) Regulations, 2016[1]

In exercise of the powers conferred by sub-section (1), and sub-clauses (*f*) and (*w*) of sub-section (2) of Section 54 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, the Unique Identification Authority of India hereby makes the following regulations, namely—

CHAPTER I
PRELIMINARY

1. Short title and commencement.—(1) These regulations may be called the Aadhaar (Authentication) Regulations, 2016.

(2) These regulations shall come into force on the date of their publication in the Official Gazette.

2. Definitions.—(1) In these regulations, unless the context otherwise requires,—

(*a*) "Act" means the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016;

(*b*) "Aadhaar number holder" means an individual who has been issued an Aadhaar number under the Act;

(*c*) "Authentication" means the process by which the Aadhaar number along with demographic information or biometric information of an individual is submitted to the Central Identities Data Repository for its verification and such Repository verifies the correctness, or the lack thereof, on the basis of information available with it;

(*d*) "Authentication facility" means the facility provided by the Authority for verifying the identity information of an Aadhaar number holder through the process of authentication, by providing a Yes/No response or e-KYC data, as applicable;

(*e*) "Authentication record" means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority thereto;

(*f*) "Authentication Service Agency" or "ASA" shall mean an entity providing necessary infrastructure for ensuring secure network connectivity and related services for enabling a requesting entity to perform authentication using the authentication facility provided by the Authority;

(*g*) "Authentication User Agency" or "AUA" means a requesting entity that uses the Yes/No authentication facility provided by the Authority;

---

1. UIDAI, Noti. No. 13012/64/2016/Legal/UIDAI (No. 3 of 2016), dated September 12, 2016, published in the Gazette of India, Extra., Part III, Section 4, dated 14th September, 2016, pp. 53-67, No. 347

(*h*) "Authority" means the Unique Identification Authority of India established under sub-section (1) of Section 11 of the Act;

(*i*) "Central Identities Data Repository" or "CIDR" means a centralised database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

(*j*) "e-KYC authentication facility" means a type of authentication facility in which the biometric information and/or OTP and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is matched against the data available in the CIDR, and the Authority returns a digitally signed response containing e-KYC data along with other technical details related to the authentication transaction;

(*k*) "e-KYC data" means demographic information and photograph of an Aadhaar number holder;

(*l*) "e-KYC User Agency" or "KUA" shall mean a requesting entity which, in addition to being an AUA, uses e-KYC authentication facility provided by the Authority;

(*m*) "License Key" is the key generated by a requesting entity as per the process laid down by the Authority;

(*n*) "PID Block" means the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication;

(*o*) "Requesting entity" means an agency or person that submits the Aadhaar number, and demographic information or biometric information, of an individual to the Central Identities Data Repository for authentication; and

(*p*) "Yes/No authentication facility" means a type of authentication facility in which the identity information and Aadhaar number securely submitted with the consent of the Aadhaar number holder through a requesting entity, is then matched against the data available in the CIDR, and the Authority responds with a digitally signed response containing "Yes" or "No", along with other technical details related to the authentication transaction, but no identity information.

(2) Words and expressions used and not defined in these regulations shall have the meaning assigned thereto under the Actor under the rules or regulations made there under or under the Information Technology Act, 2000.

CHAPTER II

AADHAAR AUTHENTICATION FRAMEWORK

3. Types of Authentication.—There shall be two types of authentication facilities provided by the Authority, namely—

(*i*) Yes/No authentication facility, which may be carried out using any of the modes specified in Regulation 4(2); and

(*ii*) e-KYC authentication facility, which may be carried out only using OTP and/or biometric authentication modes as specified in Regulation 4(2).

4. Modes of Authentication.—(1) An authentication request shall be entertained by the Authority only upon a request sent by a requesting entity electronically in accordance with these regulations and conforming to the specifications laid down by the Authority.

(2) Authentication may be carried out through the following modes:

(*a*) Demographic authentication: The Aadhaar number and demographic information of the Aadhaar number holder obtained from the Aadhaar number holder is matched with the demographic information of the Aadhaar number holder in the CIDR.

(*b*) One-time pin based authentication: A One Time Pin (OTP), with limited time validity, is sent to the mobile number and/or e-mail address of the Aadhaar number holder registered with the Authority, or generated by other appropriate means. The Aadhaar number holder shall provide this OTP along with his Aadhaar number during authentication and the same shall be matched with the OTP generated by the Authority.

(*c*) Biometric-based authentication: The Aadhaar number and biometric information submitted by an Aadhaar number holder are matched with the biometric information of the said Aadhaar number holder stored in the CIDR. This may be fingerprints-based or iris-based authentication or other biometric modalities based on biometric information stored in the CIDR.

(*d*) Multi-factor authentication: A combination of two or more of the above modes may be used for authentication.

(3) A requesting entity may choose suitable mode(s) of authentication from the modes specified in sub-regulation (2) for a particular service or business function as per its requirement, including multiple factor authentication for enhancing security. For the avoidance of doubt, it is clarified that e-KYC authentication shall only be carried out using OTP and/or biometric authentication.

5. Information to the Aadhaar number holder.—(1) At the time of authentication, a requesting entity shall inform the Aadhaar number holder of the following details—

(*a*) the nature of information that will be shared by the Authority upon authentication;

(*b*) the uses to which the information received during authentication may be put; and

(*c*) alternatives to submission of identity information.

(2) A requesting entity shall ensure that the information referred to in sub-regulation (1) above is provided to the Aadhaar number holder in local language as well.

6. Consent of the Aadhaar number holder.—(1) After communicating the information in accordance with Regulation 5, a requesting entity shall obtain the consent of the Aadhaar number holder for the authentication.

(2) A requesting entity shall obtain the consent referred to in sub-regulation (1) above in physical or preferably in electronic form and maintain logs or records of the consent obtained in the manner and form as may be specified by the Authority for this purpose.

7. Capturing of biometric information by requesting entity.—(1) A requesting entity shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by the Authority.

(2) A requesting entity shall necessarily encrypt and secure the biometric data at the time of capture as per the specifications laid down by the Authority.

(3) For optimum results in capturing of biometric information, a requesting entity shall adopt the processes as may be specified by the Authority from time to time for this purpose.

8. Devices, client applications, etc. used in authentication.—(1) All devices and equipment used for authentication shall be certified as required and as per the specifications issued, by the Authority from time to time for this purpose.

(2) The client applications i.e. software used by requesting entity for the purpose of authentication, shall conform to the standard APIs and specifications laid down by the Authority from time to time for this purpose.

9. Process of sending authentication requests.—(1) After collecting the Aadhaar number or any other identifier provided by the requesting entity which is mapped to Aadhaar number and necessary demographic and/or biometric information and/or OTP from the Aadhaar number holder, the client application shall immediately package and encrypt these input parameters into PID block before any transmission, as per the specifications laid down by the Authority, and shall send it to server of the requesting entity using secure protocols as may be laid down by the Authority for this purpose.

(2) After validation, the server of a requesting entity shall pass the authentication request to the CIDR, through the server of the Authentication Service Agency as per the specifications laid down by the Authority. The authentication request shall be digitally signed by the requesting entity and/or by the Authentication Service Agency, as per the mutual agreement between them.

(3) Based on the mode of authentication request, the CIDR shall validate the input parameters against the data stored therein and return a digitally signed Yes or No authentication response, or a digitally signed e-KYC authentication response with encrypted e-KYC data, as the case may be, along with other technical details related to the authentication transaction.

(4) In all modes of authentication, the Aadhaar number is mandatory and is submitted along with the input parameters specified in sub-regulation (1) above such that authentication is always reduced to a 1:1 match.

(5) A requesting entity shall ensure that encryption of PID Block takes place at the time of capture on the authentication device as per the processes and specifications laid down by the Authority.

10. Notification of authentication to Aadhaar number holder.—The Aadhaar number holder may be notified of any biometric and/or OTP based authentication, through the registered email and/or mobile number of the Aadhaar number holder as determined by the Authority, at the time of authentication.

11. Biometric locking.—(1) The Authority may enable an Aadhaar number holder to permanently lock his biometrics and temporarily unlock it when needed for biometric authentication.

(2) All biometric authentication against any such locked biometric records shall fail with a "No" answer with an appropriate response code.

(3) An Aadhaar number holder shall be allowed to temporarily unlock his biometrics for authentication, and such temporary unlocking shall not continue beyond the time period specified by the Authority or till completion of the authentication transaction, whichever is earlier.

(4) The Authority may make provisions for Aadhaar number holders to remove such permanent locks at any point in a secure manner.

CHAPTER III

APPOINTMENT OF REQUESTING ENTITIES AND AUTHENTICATION SERVICE AGENCIES

12. Appointment of Requesting Entities and Authentication Service Agencies.—(1) Agencies seeking to become requesting entities to use the authentication facility provided by the Authority shall apply for appointment as requesting entities in accordance with the procedure as may be specified by the Authority for this purpose. Only those entities that fulfil the criteria laid down in Schedule A are eligible to apply. The Authority may by order, amend Schedule A from time to time so as to modify the eligibility criteria.

(2) Entities seeking appointment as Authentication Service Agencies shall apply for appointment to the Authority in accordance with the procedure as may be specified by the Authority for this purpose. Only those entities that fulfil the criteria laid down in Schedule B are eligible to apply. The Authority may by order, amend Schedule B from time to time so as to modify the eligibility criteria.

(3) The Authority may require the applicant to furnish further information or clarifications, regarding matters relevant to the activity of such a requesting entity or Authentication Service Agencies, as the case may be, which may otherwise be considered necessary by the Authority, to consider and dispose of the application.

(4) The applicant shall furnish such information and clarification to the satisfaction of the Authority, within the time as may be specified in this regard by the Authority.

(5) While considering the application, the information furnished by the applicant and its eligibility, the Authority may verify the information through physical verification of documents, infrastructure, and technological support which the applicant is required to have.

(6) After verification of the application, documents, information furnished by the applicant and its eligibility, the Authority may:

a. approve the application for requesting entity or Authentication Service Agency, as the case may be; and
b. enter into appropriate agreements with the entity or agency incorporating the terms and conditions for use by requesting entities of the Authority's authentication facility, or provision of services by ASAs, including damages and disincentives for non-performance of obligations.

(7) The Authority may from time to time, determine the fees and charges payable by entities during their appointment, including application fees, annual subscription fees and fees for individual authentication transactions.

13. Procedure where application for appointment is not approved.—(1) In the event an application for appointment of requesting entity or Authentication Service Agency, as the case may be, does not satisfy the requirements specified by the Authority, the Authority may reject the application.

(2) The decision of the Authority to reject the application shall be communicated to the applicant in writing within thirty days of such decision, stating therein the grounds on which the application has been rejected.

(3) Any applicant, aggrieved by the decision of the Authority, may apply to the Authority, within a period of thirty days from the date of receipt of such intimation for reconsideration of its decision.

(4) The Authority shall reconsider an application made by the applicant and communicate its decision thereon, as soon as possible in writing.

14. Roles and responsibilities of requesting entities.—(1) A requesting entity shall have the following functions and obligations—

(*a*) establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication;
(*b*) establish network connectivity with the CIDR, through an ASA duly approved by the Authority, for sending authentication requests;
(*c*) ensure that the network connectivity between authentication devices and the CIDR, used for sending authentication requests is in compliance with the standards and specifications laid down by the Authority for this purpose;

(*d*) employ only those devices, equipment, or software, which are duly registered with or approved or certified by the Authority or agency specified by the Authority for this purpose as necessary, and are in accordance with the standards and specifications laid down by the Authority for this purpose;

(*e*) monitor the operations of its devices and equipment, on a periodic basis, for compliance with the terms and conditions, standards, directions, and specifications, issued and communicated by the Authority, in this regard, from time to time;

(*f*) ensure that persons employed by it for performing authentication functions, and for maintaining necessary systems, infrastructure and processes, possess requisite qualifications for undertaking such works;

(*g*) keep the Authority informed of the ASAs with whom it has entered into agreements;

(*h*) ensure that its operations and systems are audited by information systems auditor certified by a recognised body on an annual basis to ensure compliance with the Authority's standards and specifications and the audit report should be shared with the Authority upon request;

(*i*) implement exception-handling mechanisms and back-up identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders;

(*j*) in case of any investigation involving authentication related fraud(s) or dispute(s), it shall extend full cooperation to the Authority, or any agency appointed or authorised by it or any other authorised investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resources or information;

(*k*) in the event the requesting entity seeks to integrate its Aadhaar authentication system with its local authentication system, such integration shall be carried out in compliance with standards and specifications issued by the Authority from time to time;

(*l*) shall inform the Authority of any misuse of any information or systems related to the Aadhaar framework or any compromise of Aadhaar related information or systems within their network. If the requesting entity is a victim of fraud or identifies a fraud pattern through its fraud analytics system related to Aadhaar authentication, it shall share all necessary details of the fraud with the Authority;

(*m*) shall be responsible for the authentication operations and results, even if it sub-contracts parts of its operations to third parties. The requesting entity is also responsible for ensuring that the authentication related operations of such third party entities comply with Authority standards and specifications and that they are regularly audited by approved independent audit agencies;

may agree upon the authentication charges for providing authentication services to its customer, with such customer, and the Authority shall have

no say in this respect, for the time being; however, the Authority's right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;

(*n*) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority, for the purposes of using the authentication facilities provided by the Authority.

15. Use of Yes/No authentication facility.—(1) A requesting entity may use Yes/No authentication facility provided by the Authority for verifying the identity of an Aadhaar number holder for its own use or on behalf of other agencies.

(2) A requesting entity may permit any other agency or entity to perform Yes/No authentication by generating and sharing a separate license key for every such entity through the portal provided by the Authority to the said requesting entity. For the avoidance of doubt, it is clarified that such sharing of license key is only permissible for performing Yes/No authentication, and is prohibited in case of e-KYC authentication.

(3) Such agency or entity:

a. shall not further share the license key with any other person or entity for any purpose; and

b. shall comply with all obligations relating to personal information of the Aadhaar number holder, data security and other relevant responsibilities that are applicable to requesting entities.

(4) It shall be the responsibility of the requesting entity to ensure that any entity or agency with which it has shared a license key, complies with the provisions of the Act, regulations, processes, standards, guidelines, specifications and protocols of the Authority that are applicable to the requesting entity.

(5) The requesting entity shall be jointly and severally liable, along with the entity or agency with which it has shared a license key, for non-compliance with the regulations, processes, standards, guidelines and protocols of the Authority.

16. Use of e-KYC authentication facility.—(1) A KUA may use the e-KYC authentication facility provided by the Authority for obtaining the e-KYC data of the Aadhaar number holder for its own purposes.

(2) A KUA may perform e-KYC authentication on behalf of other agencies, and share the e-KYC data with such agency for a specified purpose, upon obtaining consent from the Aadhaar number holder for such purpose.

(3) A KUA may store, with consent of the Aadhaar number holder, e-KYC data of an Aadhaar number holder, received upon e-KYC authentication, in encrypted form and subsequently share the e-KYC data with any other agency, for a specified purpose, upon obtaining separate consent for every such sharing from the Aadhaar number holder for that purpose.

(4) The agency with whom the KUA has shared the e-KYC data of the Aadhaar number holder shall not share it further with any other entity or agency except for

completing the transaction for which the Aadhaar number holder has specifically consented to such sharing.

(5) The Aadhaar number holder may, at any time, revoke consent given to a KUA for storing his e-KYC data or for sharing it with third parties, and upon such revocation, the KUA shall delete the e-KYC data and cease any further sharing.

(6) In addition to the restriction on further sharing contained in sub-regulation (4), all other obligations relating to the personal information of the Aadhaar number holder, data security and other relevant responsibilities applicable to requesting entities, shall also apply to the agency or entity with whom e-KYC data has been shared in accordance with this Regulation 16.

(7) Upon request, a KUA shall provide a digitally signed electronic copy of the e-KYC data to the Aadhaar number holder, and the Aadhaar number holder may subsequently share the said copy with any agency:

Provided that the agency that is requesting e-KYC data from the Aadhaar number holder shall inform the purpose of doing so and take the consent of the Aadhaar number;

Provided further that the agency with whom the Aadhaar number holder has shared the e-KYC data shall not share it further with any other entity/agency except for completing the transaction for which the Aadhaar number holder specifically consented to such sharing.

(8) The KUA shall maintain auditable logs of all such transactions where e-KYC data has been shared with other agencies, for a period specified by the Authority.

17. Obligations relating to use of identity information by requesting entity.—(1) A requesting entity shall ensure that:

(*a*) the core biometric information collected from the Aadhaar number holder is not stored, shared or published for any purpose whatsoever, and no copy of the core biometric information is retained with it;

(*b*) the core biometric information collected is not transmitted over a network without creation of encrypted PID block which can then be transmitted in accordance with specifications and processes laid down by the Authority.

(*c*) the encrypted PID block is not stored, unless it is for buffered authentication where it may be held temporarily on the authentication device for a short period of time, and that the same is deleted after transmission;

(*d*) identity information received during authentication is only used for the purpose specified to the Aadhaar number holder at the time of authentication, and shall not be disclosed further, except with the prior consent of the Aadhaar number holder to whom such information relates;

(*e*) the identity information of the Aadhaar number holders collected during authentication and any other information generated during the authentication process is kept confidential, secure and protected

against access, use and disclosure not permitted under the Act and its regulations;

(*f*) the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled; and

(*g*) all relevant laws and regulations in relation to data storage and data protection relating to the Aadhaar based identity information in their systems, that of their agents (if applicable) and with authentication devices, are complied with.

18. Maintenance of logs by requesting entity.—(1) A requesting entity shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely—

(*a*) the Aadhaar number against which authentication is sought;

(*b*) specified parameters of authentication request submitted;

(*c*) specified parameters received as authentication response;

(*d*) the record of disclosure of information to the Aadhaar number holder at the time of authentication; and

(*e*) record of consent of the Aadhaar number holder for authentication,

but shall not, in any event, retain the PID information.

(2) The logs of authentication transactions shall be maintained by the requesting entity for a period of 2 (two) years, during which period an Aadhaar number holder shall have the right to access such logs, in accordance with the procedure as may be specified.

(3) Upon expiry of the period specified in sub-regulation (2), the logs shall be archived for a period of five years or the number of years as required by the laws or regulations governing the entity, whichever is later, and upon expiry of the said period, the logs shall be deleted except those records required to be retained by a court or required to be retained for any pending disputes.

(4) The requesting entity shall not share the authentication logs with any person other than the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes. The authentication logs shall not be used for any purpose other than stated in this sub-regulation.

(5) The requesting entity shall comply with all relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872, for the storage of logs.

(6) The obligations relating to authentication logs as specified in this regulation shall continue to remain in force despite termination of appointment in accordance with these regulations.

19. Roles, responsibilities and code of conduct of Authentication Service Agencies.—An Authentication Service Agency shall have the following functions and obligations—

(*a*) provide secured connectivity to the CIDR to transmit authentication request from a requesting entity in the manner as may be specified by the Authority for this purpose;

(*b*) perform basic compliance and completeness checks on the authentication data packet before forwarding it to CIDR;

(*c*) on receiving the response from CIDR, transmit the result of the transaction to the requesting entity that has placed the request;

(*d*) only engage with the requesting entities approved by the Authority and keep the Authority informed of the list of requesting entities that it serves;

(*e*) communicate to the Authority, all relevant information pertaining to any agreement that it may enter into with a requesting entity;

(*f*) ensure that the persons employed by it for performing authentication and for maintaining necessary systems, infrastructure, processes, etc., possess requisite qualifications for undertaking such works;

(*g*) ensure that its operations are audited by an information systems auditor certified by a recognized body on an annual basis, and provide a certified audit report, to the Authority, confirming its compliance with the policies, processes, procedures, standards, or specifications, issued by the Authority in this regard, from time to time;

(*h*) ensure that all infrastructure and operations including systems, processes, devices, software and biometric infrastructure, security, and other related aspects, are in compliance with the standards and specifications as may specified by the Authority for this purpose;

(*i*) at all times, comply with directions, specifications, etc. issued by the Authority, in terms of network and other Information Technology infrastructure, processes, procedures, etc.

(*j*) comply with all relevant laws and regulations relating, in particular, to data security and data management;

(*k*) any value added service that an ASA provides to a requesting entity under a contract shall not form part of the Aadhaar authentication process;

(*l*) shall be responsible to the Authority for all its authentication related operations, even in the event the ASA sub-contracts parts of its operations to other entities, the responsibility shall remain with the ASA;

(*m*) in case of investigations relating to authentication related fraud or dispute, the ASA shall extend full cooperation to the Authority (or their agency) and/or any other authorized investigation agency, including providing access to its premises, records, systems, personnel, infrastructure, any other relevant resource or information and any other relevant aspect of its authentication operations;

(*n*) may agree upon the authentication charges for providing services to a requesting entity, with such requesting entity, and the Authority shall have no say in this respect, for the time being; however, the Authority's

right to prescribe a different mechanism in this respect in the future shall be deemed to have been reserved;

(*o*) shall, at all times, comply with any contractual terms and all rules, regulations, policies, manuals, procedures, specifications, standards, and directions issued by the Authority.

20. Maintenance of logs by Authentication Service Agencies.—(1) An Authentication Service Agency shall maintain logs of the authentication transactions processed by it, containing the following transaction details, namely—

(*a*) identity of the requesting entity;

(*b*) parameters of authentication request submitted; and

(*c*) parameters received as authentication response:

Provided that no Aadhaar number, PID information, device identity related data and e-KYC response data, where applicable shall be retained.

(2) Authentication logs shall be maintained by the ASA for a period of 2 (two) years, during which period the Authority and/or the requesting entity may require access to such records for grievance redressal, dispute redressal and audit in accordance with the procedure specified in these regulations. The authentication logs shall not be used for any purpose other than stated in this sub-regulation.

(3) Upon expiry of the period specified in sub-regulation (2), the authentication logs shall be archived for a period of five years, and upon expiry of the said period of five years or the number of years as required by the laws or regulations governing the entity whichever is later, the authentication logs shall be deleted except those logs required to be retained by a court or which are required to be retained for any pending disputes.

(4) The ASA shall comply with all applicable laws in respect of storage and maintenance of these logs, including the Information Technology Act, 2000.

(5) The obligations relating to authentication logs as specified in this regulation shall continue to remain in force despite termination of appointment in accordance with these regulations.

21. Audit of requesting entities and Authentication Service Agencies.—(1) The Authority may undertake audit of the operations, infrastructure, systems and procedures, of requesting entities, including the agencies or entities with whom they have shared a license key or the entities on whose behalf they have performed authentication, and Authentication Service Agencies, either by itself or through audit agencies appointed by it, to ensure that such entities are acting in compliance with the Act, rules, regulations, policies, procedures, guidelines issued by the Authority.

(2) The Authority may conduct audits of the operations and systems of the entities referred to in sub-regulation (1), either by itself or through an auditor appointed by the Authority. The frequency, time and manner of such audits shall be as may be notified by the Authority from time to time.

(3) An entity subject to audit shall provide full co-operation to the Authority or any agency approved and/or appointed by the Authority in the audit process, and provide to the Authority or any agency approved and/or appointed by the Authority, complete access to its procedures, records and information pertaining to services availed from the Authority. The cost of audits shall be borne by the concerned entity.

(4) On identification of any deficiency by the Authority, the Authority may require the concerned entity to furnish necessary clarifications and/or information as to its activities and may also require such entity either to rectify the deficiencies or take action as specified in these regulations.

22. Data Security.—(1) Requesting entities and Authentication Service Agencies shall have their servers used for Aadhaar authentication request formation and routing to CIDR to be located within data centres located in India.

(2) Authentication Service Agency shall establish dual redundant, secured leased lines or MPLS connectivity with the data centres of the Authority, in accordance with the procedure and security processes as may be specified by the Authority for this purpose.

(3) Requesting entities shall use appropriate license keys to access the authentication facility provided by the Authority only through an ASA over secure network, as may be specified by the Authority for this purpose.

(4) Requesting Entities and Authentication Service Agencies shall adhere to all regulations, information security policies, processes, standards, specifications and guidelines issued by the Authority from time to time.

23. Surrender of the access to authentication facility by requesting entity or Authentication Service Agency.—(1) A Requesting Entity or ASA, appointed under these regulations, desirous of surrendering the access to the authentication facility granted by Authority, may make a request for such surrender to the Authority.

(2) While disposing such surrender request under these regulations, the Authority may require the requesting entity or ASA to satisfy the Authority about any matter necessary for smooth discontinuance or termination of services, including–

(*a*) the arrangements made by the requesting entity for maintenance and preservation of authentication logs and other documents in accordance with these regulations and procedures as may be specified by the Authority for this purpose;

(*b*) the arrangements made by the requesting entity for making authentication record available to the respective Aadhaar number holder on such request;

(*c*) records of redressal of grievances, if any;

(*d*) settlement of accounts with the Authority, if any;

(*e*) in case of surrender by ASAs, the ASA, prior to the surrender of its access, shall ensure that its associated requesting entities are given adequate time to migrate to other ASAs in operation.

24. Agencies appointed before commencement of these regulations.—(1) Any Authentication User Agency (AUA) or e-KYC User Agency (KUA), appointed prior to the commencement of these regulations shall be deemed to be a requesting entity, and any Authentication Service Agency (ASA) or e-KYC Service Agency (KSA) shall be deemed to be an Authentication Service Agency, under these regulations, and all the agreements entered into between such agencies and the Unique Identification Authority of India, established vide notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority shall continue to be in force to the extent not inconsistent with the provisions of the Act, these regulations, and other regulations, policies, processes, procedures, standards and specifications issued by the Authority.

(2) Notwithstanding anything contained in sub-regulation (1), any deemed requesting entity or Authentication Service Agency referred to in sub-regulation (1) shall be required to comply with the provisions of the Act, these regulations, other regulations framed by the Authority, and the policies, processes, procedures, standards and specifications issued by the Authority.

(3) In the event any such agency referred to in sub-regulation (1) seeks to discontinue using the authentication facility as specified in these regulations, it may immediately make an application for termination of its credentials and stop its functions forthwith:

Provided that in such cases, no compensation shall be payable to the agency or to the Authority upon such termination.

(4) On discontinuance under sub-regulation (3), the concerned entity shall be required to comply with the closure requirements listed in Regulation 23(2).

25. Liability and action in case of default.—(1) Where any requesting entity or an ASA appointed under the Act,—

(*a*) fails to comply with any of the processes, procedures, standards, specifications or directions issued by the Authority, from time to time;

(*b*) is in breach of its obligations under the Act and these regulations;

(*c*) uses the Aadhaar authentication facilities for any purpose other than those specified in the application for appointment as requesting entity or ASA,

(*d*) fails to furnish any information required by the Authority for the purpose of these regulations; or

(*e*) fails to cooperate in any inspection or investigation or enquiry or audit conducted by the Authority,

the Authority may, without prejudice to any other action which may be taken under the Act, take such steps to impose disincentives on the requesting entity or an ASA for contravention of the provisions of the Act, rules and regulations

thereunder, including suspension of activities of such entity or agency, or other steps as may be more specifically provided for in the agreement entered into by such entities with the Authority:

Provided that the entity or agency shall be given the opportunity of being heard before the termination of appointment and discontinuance of its operations relating to Aadhaar authentication.

(2) Any such action referred to in sub-regulation (1) may also be taken against any entity or agency with which an AUA has shared its license key for Yes/No authentication and any entity with which a KUA has shared e-KYC data.

(3) Upon termination of appointment by the Authority, the requesting entity or the ASA shall, forthwith, cease to use the Aadhaar name and logo for any purposes, and in any form, whatsoever, and may be required to satisfy the Authority of necessary aspects of closure, including those enumerated in Regulation 23(2).

CHAPTER IV

AUTHENTICATION TRANSACTION DATA AND AUTHENTICATION RECORDS

[2][**26. Storage and Maintenance of Authentication Transaction Data.**—(1) The Authority shall store and maintain authentication transaction data, which shall contain the following information—

(*a*) authentication request data received including PID block;

(*b*) authentication response data sent;

(*c*) meta data related to the transaction;

(*d*) any authentication server side configurations as necessary:

Provided that the Authority shall not, in any case, store the purpose of authentication.

CASE LAW ▸ Validity.—Held impermissible in the present form in *K.S. Puttaswamy* v. *Union of India* (Aadhaar - 5 J.), 2018 SCC OnLine SC 1642 in the following terms—

> "There is a need to amend Regulation 26 to restrict it to process meta data, and to exclude other type of meta data specifically. Metabase relating to transaction, as provided in Regulation 26 in the present form, is held to be impermissible, which needs suitable amendment."

27. Duration of storage.—[3][(1) Authentication transaction data shall be retained by the Authority for a period of 6 months, and thereafter archived for a period of five years.]

(2) Upon expiry of the period of five years specified in sub-regulation (1), the authentication transaction data shall be deleted except when such authentication transaction data are required to be maintained by a court or in connection with any pending dispute.

---

2. Held impermissible in the present form in *K. S. Puttaswamy* v. *Union of India* (Aadhaar - 5 J.), 2018 SCC OnLine SC 1642.
3. Held invalid in *K. S. Puttaswamy* v. *Union of India* (Aadhaar - 5 J.), 2018 SCC OnLine SC 1642.

CASE LAW ▸ Validity.—Regulation 27(1), Held invalid in *K.S. Puttaswamy* v. *Union of India* (Aadhaar - 5 J.), 2018 SCC OnLine SC 1642 in the following terms—

"Authentication records are not to be kept beyond a period of six months, as stipulated in Regulation 27(1) of the Authentication Regulations. This provision which permits records to be archived for a period of five years is held to be bad in law."

28. Access by Aadhaar number holder.– -(1) An Aadhaar number holder shall have the right to access his authentication records subject to conditions laid down and payment of such fees as prescribed by the Authority by making requests to the Authority within the period of retention of such records before they are archived.

(2) The Authority may provide mechanisms such as online portal or mobile application or designated contact centers for Aadhaar number holders to obtain their digitally signed authentication records within the period of retention of such records before they are archived as specified in these regulations.

(3) The Authority may provide digitally signed e-KYC data to the Aadhaar number holder through biometric or OTP authentication, subject to payment of such fees and processes as specified by the Authority.

(4) The authentication records and e-KYC data shall not be shared with any person or entity:

(*a*) other than with the Aadhaar number holder to whom the records or e-KYC data relate in accordance with the verification procedure specified. Aadhaar number holder may share their digitally signed authentication records and e-KYC data with other entities which shall not further share with any other agencies without obtaining consent of the Aadhaar holder every time before such sharing.

(*b*) except in accordance with the Act.

CHAPTER V

MISCELLANEOUS

29. Savings.—All procedures, orders, processes, standards, specifications and policies issued and MOUs, agreements or contracts entered by the Unique Identification Authority of India, established vide notification of the Government of India in the Planning Commission number A-43011/02/2009-Admin. I, dated the 28th January, 2009 or any officer of such authority, prior to the establishment of the Authority under the Act shall continue to be in force to the extent that they are not inconsistent with the provisions of the Act and regulations framed thereunder.

30. Power to issue clarifications, guidelines and removal of difficulties.— In order to remove any difficulties or clarify any matter pertaining to application or interpretation of these regulations, the Authority may issue clarifications and guidelines in the form of circulars.

SCHEDULE A

Eligibility criteria for appointment as requesting entities

[*See* Regulation 10(1)]

1. Entities seeking to use authentication facility provided by the Authority as requesting entities are classified under following categories for appointment as Authentication User Agency (AUA) and/or e-KYC User Agency (KUA), as the case may be:

Sl. No.	Organisation Category
Category 1	Government Organisation
1.1	A Central/State Government Ministry/Department and their attached or subordinate offices.
1.2	An undertaking owned and managed by Central/State Government (PSU)
1.3	An Authority constituted under the Central/State Act/Special Purpose Organisation constituted by Central/State government.
Category 2	Regulated Service Providers
2.1	Regulated/Licensed by RBI.—Banks and Payment & Settlement System
	2.1.1 Public Sector Banks (PSB)
	2.1.2 Private Banks, Foreign Banks Licensed by RBI to operate in India, Payment Banks, Small Finance Banks
	2.1.3 Regional Rural Banks
	2.1.4 Co-operative Banks
	5. State Co-operative Banks 6. District Co-operative Banks 7. Scheduled Urban Cop-operatives Banks 8. Non Scheduled Urban Co-operative Banks
	2.1.5 Payment & Settlement System Network 1. Financial market infrastructure 2. Retails payments Organisation 3. Cards payment network 4. ATM networks 5. Pre-paid payment instruments 6. White label ATM operators 7. Instant Money Transfer
	2.1.6 Non-Banking Financial Company
2.2	Regulated by IRDA/PFRDA.—Financial Institutions
2.3	Regulated by TRAI.—Telecom
2.4	Regulated by CCA.—Certifying Authority, Digital Locker providers, e-Sign providers

2.5	Regulated by SEBI. –KYC Registration Agency (KRA), Depository Participant (DP), Asset Management Company (AMC), Trading Exchanges, Registrar and Transfer Agents	
2.6	Regulated by National Housing Bank	
Category 3	Other Entities	
3.1	3.1.1	Company registered in India under the Companies Act, 1956/The Companies Act, 2013 (Company under group of companies has to apply individually)
	3.1.2	Partnership registered under the Indian Partnership Act, 1932 or under the Limited Liability Partnership Act, 2008
	3.1.3	Proprietorship firm
	3.1.4	Not-for-profit Organisations (under Section 25 under The Companies Act, 1956)
	3.1.5	Academic Institutions/Research and Development Organisations
	3.1.6	Societies registered under Indian Societies Registration Act, 1860 or the Indian Trust Act, 1882 or the Companies Act, 2013 (Sec 8)/the Co-operative Societies Act, 1912
	3.1.7	Any entity other than above mentioned categories

2. Technical and Financial criteria for entities for appointment as requesting entity are as under—

Category	Authentication User Agency (AUA)		Additional requirements for eKYC User Agency (KUA)
	Technical Requirements	Financial Requirements	
Category 1	1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India.	No financial requirement	No additional requirement for KUA
Category 2		No financial requirement	No additional requirement for KUA
	2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transactions per month. 3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy. 4. Organisation should have adopted data security requirements as per the IT Act, 2000.		

Category 3	1. Backend infrastructure, such as servers, databases etc. of the entity, required specifically for the purpose of Aadhaar authentication, should be located within the territory of India. 2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transaction per month. 3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy. 4. Organisation should have adopted Data security requirements as per the IT Act, 2000. 5. Entity should be in business for minimum of 1 year from date of commencement of Business.	1. Paid up capital of minimum 1 (one) Crore. OR Annual turnover of minimum 5 (Five) Crore during the last Financial year.	Entity should meet Authentication Transaction Criteria as laid down by the Authority from time to time.

SCHEDULE B

Eligibility criteria of Authentication Service Agencies

[*See* Regulation 10(2)]

1. Entities seeking to provide secure access to CIDR to requesting entities for enabling authentication services are classified under following categories for appointment as Authentication Service Agency:

Sl. No	Organisation Category
Category 1	A Central/State Government Ministry/Department or an undertaking owned and managed by Central/State Government
Category 2	An Authority constituted under the Central/State Act
Category 3	Any other entity of national importance as determined by the Authority
Category 4	A company registered in India under the Indian Companies Act, 1956
Category 5	AUA/KUA

2. Technical and Financial criteria for entities for appointment as Authentication Service Agency are as under—

Category	Financial Requirement	Technical Requirement
Category 1, 2 and 3	No financial requirements	No technical requirements
Category 4	An annual turnover of at least 100 crores in last three financial years	A Telecom Service Provider (TSP) including All Unified Licensees (having Access Service Authorization)/Unified Licensees (AS)/Unified

		Access Services Licensees/Cellular Mobile Telephone Service Licensees operating pan-India fiber optics network and should have a minimum of 100 MPLS Points of Presence (PoP) across all states Or Should be a Network Service Provider (NSP) or System Integrator having pan-India network connectivity for data transmission and should have 100 MPLS PoPs in India,
Category 5	No Financial requirements	Any AUA or KUA meeting authentication transaction criteria as laid down by the Authority from time to time

NOTIFICATION

UIAI, Noti. No. 13012/79/2017/Legal-UIDAI (No. 4 of 2017), dated July 14, 2017, published in the Gazette of India, Extra., Part III, Section 4, dated 14th July, 2017, pp. 2-3, No. 284.

In exercise of Regulation 12-A of the Aadhaar (Enrolment and Update) (Second Amendment) Regulations, 2017 (No. 2 of 2017) and the Aadhaar (Enrolment and Update) (Third Amendment) (No. 3 of 2017), the Unique Identification Authority of India (UIDAI) hereby issues the following notification, namely:—

1. Whereas the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"), and Regulations framed thereunder the Aadhaar Act have come into effect from 14th September, 2016 and notifications to this effect have been published in the Official Gazette,

2. And Whereas the Prevention of Money Laundering (Maintenance of Records) Rules, 2005 ("PML Rules, 2005") have been amended with effect from June 1, 2017 to require Aadhaar for every bank account. All existing Bank accounts have to be verified with Aadhaar by the banks by 31st December, 2017, failing which the accounts will become inoperative,

3. And Whereas Regulation 12-A of the Aadhaar (Enrolment and Update) (Second Amendment) Regulations, 2017 (No. 2 of 2017) and the Aadhaar (Enrolment and Update) (Third Amendment) (No. 3 of 2017) provides that:

> "12-A. *Entities requiring Aadhaar as condition for fulfillment of any obligation, etc.*—The Authority may require any Central or State department or agency or any Scheduled Bank or any other entity which requires an individual to undergo authentication or furnish proof of possession of Aadhaar number as a condition for receipt of any subsidy, benefit, service or fulfillment of any obligation pursuant to any Act or Rule or Regulation or order made thereunder, to ensure enrolment of such individual who is yet to be enrolled or update their Aadhaar details, by setting up enrolment centres at their premises.".

4. And Whereas there are more than 100 Crore bank accounts which will be required to be verified before the aforesaid date and every new customer will also be required to be verified with Aadhaar,

5. And Whereas Scheduled Commercial Banks have major share of bank account holders who will need to authenticate their bank accounts with their Aadhaar numbers,

6. Therefore, it is necessary to provide Aadhaar enrolment and update facilities in Scheduled Commercial Banks so that no undue hardship is caused to their customers owing to the aforesaid amendment of the PML Rules, 2005,

7. And Therefore Unique Identification Authority of India, in exercise of Regulation 12A of the Aadhaar (Enrolment and Update) (Second Amendment) Regulations, 2017 (No. 2 of 2017) and

the Aadhaar (Enrolment and Update) (Third Amendment) (No. 3 of 2017), hereby directs that every Scheduled Commercial Bank shall provide Aadhaar enrolment and update facilities to its customers in the following manner:

i. Every Scheduled Commercial Bank shall set up Aadhaar enrolment and update facility inside its bank premises at a minimum of 1 out of their every 10 branches by 30th August, 2017.

ii. The selection of branches for enrolment and update facility shall be such that it covers all the district headquarters where it is present, and that there is maximum coverage of Talukas/Block in every district.

iii. The Scheduled Commercial Bank shall notify to its customers, the general public, and UIDAI of the locations of branches where Aadhaar enrolment and update facilities will be provided by them. The list of such branches shall be displayed on its websites. Any changes in locations shall be notified at the earliest in the aforesaid manner.

iv. The Banks may at its discretion provide the Aadhaar Enrolment and Update facility to customers of other banks.

v. The Bank may charge the customers for the Aadhaar enrollment and update services at the rate prescribed by UIDAI.

vi. The Scheduled Commercial Bank shall, if not already done so, become Registrar of UIDAI for providing enrolment and update facilities.

8. Any non-compliance of these directions shall be dealt under Section 42 of the Aadhaar Act.