Finahub Technology Solutions Pvt Ltd.
Kinfra Hi-Tech Park, HMT Colony PO, Kalamassery. Kochi.
www.finahub.com

Violation of these aadhaar regulations will be really costly for you

Recently UIDAI introduced a list of Aadhaar regulations and agreement terms that a KUA/AUA should not violate. These regulations are to be strictly followed by the organizations, otherwise, a fine of 1 lakh to 3 lakh will be issued per day. The relevant regulations and agreements are given below.

Regulation Number	Regulation
5(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(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.
7(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.
8(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.
8(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(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.
9(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.
14 (1)(a)	A requesting entity shall have the following functions and obligations:— Establish and maintain necessary authentication related operations, including own systems, processes, infrastructure, technology, security, etc., which may be necessary for performing authentication;
14 (1) (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;
14 (1) (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;
14 (1)(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,
14 (1) (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.
14 (1) (g)	Keep the Authority informed of the ASAs with whom it has entered into agreements;
14 (1) (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;
14(1) (i)	Implement exception-handling mechanisms and backup identity authentication mechanisms to ensure seamless provision of authentication services to Aadhaar number holders;

14(1) (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;
14(1) (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;
14 (1) (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;
14(1) (m)	Shall be responsible for the authentication operations and results, even if it subcontracts 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;
14(1) (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 (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.
15 (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.
15 (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.

16 (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.
16 (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.
16 (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.
16 (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.
16 (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 (1)(a)	A requesting entity shall ensure that 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;
17 (1) (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.
17 (1) (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;
17 (1) (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;
17 (1) (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;
17 (1) (f)	the private key used for digitally signing the authentication request and the license keys are kept secure and access controlled;

17 (1) (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 (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.
18 (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.
18 (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.
18 (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.
18 (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.
18 (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.
21 (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.

22 (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.
22 (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.
Agreement Term #	**Agreement Term Text**
2.1	UIDAI hereby grants the Authentication User Agency a non-exclusive and revocable right to use Aadhaar Authentication Services, for providing such Aadhaar Enabled Services to Aadhaar Number Holder(s) as set out in the appointment letter and in the manner set out in this Agreement. The Authentication User Agency understands and agrees that it shall be responsible to UIDAI for all its Aadhaar authentication related aspects, covered by this Agreement.
2.2	In the event the Authentication User Agency outsources part(s) of its operations to other entities, the ultimate responsibility for the results of Aadhaar authentication related operations lies with the Authentication User Agency, and the Authentication User Agency shall ensure that the entity to which it has outsourced its operations is audited annually by information systems auditor certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI.
2.3	The Authentication User Agency shall ensure that the client application to be used by Sub AUA for Aadhaar authentication is developed and digitally signed by Authentication User Agency or else Authentication User Agency shall give its digitally signed SDK to Sub AUA for the purposes of capturing Aadhaar number and other authentication details such as demographics, OTP or biometrics. Under no circumstances, Sub AUA shall capture Aadhaar number and other authentication data for the purposes of Aadhaar Authentication by any means other than these two means described above. In addition, under no circumstances Authentication User Agency shall expose the Aadhaar Authentication API directly to any other agency or application and only Authentication User Agency provided client application or SDK must access these APIs in a secure fashion. The Authentication User Agency shall also ensure that the Sub AUA client application or SDK, as the case may be, used for Aadhaar Authentication, is audited at the time of creation of the application/SDK and also for every major release of the application/SDK or every year thereafter whichever comes first, by information systems auditor(s) certified by STQC / CERT-IN and compliance audit report is submitted to UIDAI.

2.5	It is hereby mutually agreed between the Parties that the rights and obligations of the Authentication User Agency, under this Agreement, are non-transferable and non-assignable whether by sale, merger, or by operation of law, except with the express written consent of UIDAI.
2.6	The Authentication User Agency hereby unequivocally agrees that the use of the Aadhaar Authentication Services by it for providing Aadhaar Enabled Services to Aadhaar Number Holder(s) and the Aadhaar Authentication Services shall not, in any manner, whether direct or indirect, be used for purposes that are anti government or anti-State or discriminatory or related to money laundering or in contravention of any laws applicable in India.
3.1	The Authentication User Agency shall take permission of UIDAI before entering into any agreement with any Sub AUA and shall duly register them in the manner prescribed by UIDAI from time to time. The Authentication User Agency shall share a separate license key with each Sub AUA. The Authentication User Agency shall also issue a unique Sub AUA code to identify each Sub AUA and shall include the Sub AUA code in all authentication requests originating from that Sub AUA which it forwards to CIDR for authentication.

4	4.1 The Authentication User Agency is aware that “Aadhaar” is the intellectual property of UIDAI and the Authentication User Agency understands that any unauthorized reproduction of the same constitutes infringement and may be subject to penalties, both civil and criminal. 4.2 It is hereby mutually agreed between the Parties that the Authentication User Agency shall have a non-exclusive right to use the Aadhaar name and logo and to represent itself as an entity providing Aadhaar Enabled Services to Aadhaar Number Holder(s), subject to the condition that all rights, title and interest, including intellectual property rights, in the Aadhaar name and logo shall vest, at all times, either during the operation of this Agreement or otherwise, in UIDAI. Page 6 of 13 4.3 The Authentication User Agency hereby unequivocally agrees that it shall use the Aadhaar name and logo, without any modification, in its promotional, educational and informational literature, for the duration of this Agreement. 4.4 The Authentication User Agency hereby unequivocally agrees that it shall not authorize any other entity or individual to use the Aadhaar name and logo, except with the prior written permission of UIDAI. 4.5 The Authentication User Agency hereby unequivocally agrees that upon becoming aware of unauthorized use, copy, infringement or misuse of the Aadhaar name and/or logo, and any rights, title and interest therein, including intellectual property rights, it shall notify UIDAI about such unauthorized use forthwith. At the request of UIDAI, the Authentication User Agency shall take part in or give assistance in respect of any legal proceedings and execute any documents and do any things reasonably necessary to protect the rights, title and interest of UIDAI, including intellectual property rights, in respect of the Aadhaar name and logo.
6.1	The Authentication User Agency and all its Sub AUAs shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall keep the same confidential, maintain secrecy of all such information of confidential nature and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake.
6.2	The Authentication User Agency hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Authentication User Agency, as a result of operation of this Agreement, is secured and protected against any loss or unauthorised access or use or unauthorised disclosure thereof, including all obligations relating to protection of information in the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016.

8.1	The Authentication User Agency shall set up grievance handling mechanism to receive and address the complaints from the Aadhaar Number Holders with regard to authentication services performed by it. It shall be the responsibility of the Authentication User Agency to ensure that similar mechanism is set up by its sub-AUAs.
8.3	UIDAI may require from the Authentication User Agency the details of any complaint and its redressal by the Authentication User Agency.
8.4	The Authentication User Agency shall provide a quarterly report of all the grievances handled by it in the format prescribed by UIDAI, from time to time.