THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

(18 of 2016)

[25th March, 2016]

An Act to provide for, as a good governance, efficient, transparent, and targeted delivery of subsidies, benefits and services, the expenditure for which is incurred from the Consolidated Fund of India or the Consolidated Fund of the State, to individuals residing in India through assigning of unique identity numbers to such individuals and for matters connected therewith or incidental thereto.

Be it enacted by Parliament in the Sixty-seventh Year of the Republic of India as follows:

CHAPTER I

PRELIMINARY

1. Short title, extent and commencement.—(1) This Act may be called the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

(2) It shall extend to the whole of India and save as otherwise provided in this Act, it shall also apply to any offence or contravention committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

2. Definitions.—In this Act, unless the context otherwise requires,—

(a) “Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3, and includes any alternative virtual identity generated under sub-section (4) of that section;

(aa) “Aadhaar ecosystem” includes enrolling agencies, Registrars, request entities, offline verification-seeking entities and any other entity or group of entities as may be specified by regulations;

(b) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under this Act;

(ba) “Adjudicating Officer” means an adjudicating officer appointed under sub-section (1) of section 33B;

(bb) “Appellate Tribunal” means the Appellate Tribunal referred to in sub-section (1) of section 33C;

(c) “authentication” means the process by which the Aadhaar number along with demographic information or biometric information of an

---

2. Ins. by Act 14 of 2019, sec. 2 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
3. The words “except the State of Jammu and Kashmir” omitted by the Jammu and Kashmir Reorganisation Act, 2019 (34 of 2019), secs. 85, 96 and Fifth Sch., Table-1 [w.e.f. 31-10-2019].
5. Subs. by Act 14 of 2019, sec. 30(i), for clause (a) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019]. Clause (a), before substitution, stood as under:
   (a) “Aadhaar number” means an identification number issued to an individual under sub-section (3) of section 3.
6. Ins. by Act 14 of 2019, sec. 30(iii) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
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 record" means the record of the time of authentication and identity of the requesting entity and the response provided by the Authority thereto;

(e) "Authority" means the Unique Identification Authority of India established under sub-section (1) of section 11;

(f) "benefit" means any advantage, gift, reward, relief, or payment, in cash or kind, provided to an individual or a group of individuals and includes such other benefits as may be notified by the Central Government;

(g) "biometric information" means photograph, fingerprint, iris scan, or other such biological attributes of an individual as may be specified by regulations;

(h) "Central Identities Data Repository" 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;

(i) "Chairperson" means the Chairperson of the Authority appointed under section 12;

(j) "child" means a person who has not completed eighteen years of age;

(k) "core biometric information" means fingerprint, iris scan, or such other biological attribute of an individual as may be specified by regulations;

(l) "demographic information" includes information relating to the name, date of birth, address and other relevant information of an individual, as may be specified by regulations for the purpose of issuing an Aadhaar number, but shall not include race, religion, caste, tribe, ethnicity, language, records of entitlement, income or medical history;

(m) "enrolling agency" means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under this Act;

(n) "enrolment" means the process, as may be specified by regulations, to collect demographic and biometric information from individuals by the enrolling agencies for the purpose of issuing Aadhaar numbers to such individuals under this Act;

(o) "identity information" in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information;

(p) "notification" means a notification published in the Official Gazette and the expression "notified" with its cognate meanings and grammatical variations shall be construed accordingly;

1. Ins. by Act 44 of 2019, sec. 3(iv) [w.e.f. 25-7-2019, vide S.O. 2644(E), dated 25th July, 2019].
1. "Offline verification" means the process of verifying the identity of the Aadhaar number holder without authentication, through such offline modes as may be specified by regulations;]

1. "Offline verification-seeking entity" means any entity desirous of undertaking offline verification of an Aadhaar number holder;

(q) "prescribed" means prescribed by rules made by the Central Government under this Act;

(r) "records of entitlement" means records of benefits, subsidies or services provided to, or availed by, any individual under any programme;

(s) "Registrar" means any entity authorised or recognised by the Authority for the purpose of enrolling individuals under this Act;

(t) "regulations" means the regulations made by the Authority under this Act;

(u) "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;

(v) "resident" means 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;

(w) "service" means any provision, facility, utility or any other assistance provided in any form to an individual or a group of individuals and includes such other services as may be notified by the Central Government;

(x) "subsidy" means any form of aid, support, grant, subvention, or appropriation, in cash or kind, to an individual or a group of individuals and includes such other subsidies as may be notified by the Central Government.

CHAPTER II

ENROLMENT

3. Aadhaar number.—(1) Every resident shall be entitled to obtain an Aadhaar number by submitting his demographic information and biometric information by undergoing the process of enrolment:

Provided that the Central Government may, from time to time, notify such other category of individuals who may be entitled to obtain an Aadhaar number.

(2) The enrolling agency shall, at the time of enrolment, inform the individual undergoing enrolment of the following details in such manner as may be specified by regulations, namely:—

(a) the manner in which the information shall be used;

(b) the nature of recipients with whom the information is intended to be shared during authentication; and

1. Ins. by Act 14 of 2019, sec. 3(v) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
(c) the existence of a right to access information, the procedure for
making requests for such access, and details of the person or
department in-charge to whom such requests can be made.

(3) On receipt of the demographic information and biometric information under
sub-section (1), the Authority shall, after verifying the information, in such manner
as may be specified by regulations, issue an Aadhaar number to such individual.

(4) The Aadhaar number issued to an individual under sub-section (3)
shall be a twelve-digit identification number and any alternative virtual identity
as an alternative to the actual Aadhaar number of an individual that shall be
generated by the Authority in such manner as may be specified by regulations.

NOTIFICATION

In exercise of the powers conferred by proviso to sub-section (1) of section 3 of the
Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act,
2016 (18 of 2016), the Central Government hereby notifies that a Non Resident Indian,
after his arrival in India, shall be entitled to obtain an Aadhaar number.

Explanation.—For the purposes of this notification, “Non Resident Indian” means a
person who is a citizen of India holding a valid Indian Passport but not a resident as
defined under clause (v) of section 2 of the said Act.

2. This notification shall come into force from the date of publication in the official
Gazette.

[Vide S.O. 3425(E), dated 20th September, 2019, published in the Gazette of India,
Extra., Pt. II, Sec. 3(ii), No. 3119, dated 20th September, 2019.]

3A. Aadhaar number of children.—(1) The enrolling agency shall, at the time
of enrolment of a child, seek the consent of the parent or guardian of the child, and
inform the parent or guardian, the details specified under sub-section (2) of section 3.

(2) A child who is an Aadhaar number holder may, within a period of
six months of attaining the eighteen years of age, make an application to the
Authority for cancellation of his Aadhaar number, in such manner as may be
specified by regulations and the Authority shall cancel his Aadhaar number.

(3) Notwithstanding anything in section 7, a child shall not be denied any
subsidy, benefit or service under that section in case of failure to establish his
identity by undergoing authentication, or furnishing proof of possession of
Aadhaar number, or in the case of a child to whom no Aadhaar number has
been assigned, producing an application for enrolment.

4. Properties of Aadhaar number.—(1) An Aadhaar number, issued to an
individual shall not be re-assigned to any other individual.

(2) An Aadhaar number shall be a random number and bear no relation to
the attributes or identity of the Aadhaar number holder.

3(3) Every Aadhaar number holder to establish his identity, may voluntarily
use his Aadhaar number in physical or electronic form by way of authentication

1. Ins. by Act 14 of 2019, sec. 4 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
2. Ins. by Act 14 of 2019, sec. 5 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
3. Ins. by S.O. 411(E), dated 19th January, 2018; Sub-section (3), before substitution, stood as under:

“(3) An Aadhaar number, in physical or electronic form subject to authentication and
other conditions, as may be specified by regulations, may be accepted as proof of identity of
the Aadhaar number holder for any purpose.

Explanation.—For the purposes of this sub-section, the expression “electronic form” shall
have the same meaning as assigned to it in clause (c) of sub-section (1) of section 2 of the
Information Technology Act, 2000 (21 of 2000).”
or offline verification, or in such other form as may be notified, in such manner as may be specified by regulations.

Explanation.—For the purposes of this section, voluntary use of the Aadhaar number by way of authentication means the use of such Aadhaar number only with the informed consent of the Aadhaar number holder.

(4) An entity may be allowed to perform authentication, if the Authority is satisfied that the requesting entity is—

(a) compliant with such standards of privacy and security as may be specified by regulations; and

(b) (i) permitted to offer authentication services under the provisions of any other law made by Parliament; or

(ii) seeking authentication for such purpose, as the Central Government in consultation with the Authority, and in the interest of State, may prescribe.

(5) The Authority may, by regulations, decide whether a requesting entity shall be permitted the use of the actual Aadhaar number during authentication or only an alternative virtual identity.

(6) Every requesting entity to whom an authentication request is made by an Aadhaar number holder under sub-section (3) shall inform to the Aadhaar number holder of alternate and viable means of identification and shall not deny any service to him for refusing to, or being unable to, undergo authentication.

(7) Notwithstanding anything contained in the foregoing provisions, mandatory authentication of an Aadhaar number holder for the provision of any service shall take place if such authentication is required by a law made by Parliament.

5. Special measures for issuance of Aadhaar number to certain category of persons.—The Authority shall take special measures to issue Aadhaar number to women, children, senior citizens, persons with disability, unskilled and unorganised workers, nomadic tribes or to such other persons who do not have any permanent dwelling house and such other categories of individuals as may be specified by regulations.

6. Update of certain information.—The Authority may require Aadhaar number holders to update their demographic information and biometric information, from time to time, in such manner as may be specified by regulations, so as to ensure continued accuracy of their information in the Central Identities Data Repository.

CHAPTER III

AUTHENTICATION

7. Proof of Aadhaar number necessary for receipt of certain subsidies, benefits and services, etc.—The Central Government or, as the case may be, the State Government may, for the purpose of establishing identity of an individual as a condition for receipt of a subsidy, benefit or service for which the expenditure is incurred from, or the receipt therefrom forms part of, the Consolidated Fund of India [or the Consolidated Fund of State], require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case

1. Ins. by Act 14 of 2019, sec. 7 [w.e.f. 25.7.2019, vide S.O. 2649(E), dated 25th July, 2019].
of an individual to whom no Aadhaar number has been assigned, such individual makes an application for enrolment:

Provided that if an Aadhaar number is not assigned to an individual, the individual shall be offered alternate and viable means of identification for delivery of the subsidy, benefit or service.

8. Authentication of Aadhaar number.—(1) The Authority shall perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information or demographic information, subject to such conditions and on payment of such fees and in such manner as may be specified by regulations.

(2) A requesting entity shall—

(a) unless otherwise provided in this Act, obtain the consent of an individual or, in the case of a child, obtain the consent of his parent or guardian before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations; and

(b) ensure that the identity information of an individual is only used for submission to the Central Identities Data Repository for authentication:

Provided that the requesting entity shall, in case of failure to authenticate due to illness, injury or infirmity owing to old age or otherwise or any technical or other reasons, provide such alternate and viable means of identification of the individual, as may be specified by regulations.

(3) A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, or in the case of a child, his parent or guardian, the following details with respect to authentication, namely:

(a) the nature of information that may be shared upon authentication;

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

(c) alternatives to submission of identity information to the requesting entity.

(4) The Authority shall respond to an authentication query with a positive, negative or any other appropriate response, sharing such identity information excluding any core biometric information.

COMMENTS

(Based on Notes on Clauses of the Bill)

This section empowers the Authority to perform authentication of the Aadhaar number of an Aadhaar number holder submitted by any requesting entity, in relation to his biometric information and demographic information subject to such conditions and on payment of such fees and in such manner as specified by regulations. It is provided that the entity shall unless otherwise provided in this Act, obtain the consent of an individual before collecting his identity information for the purposes of authentication in such manner as may be specified by regulations and to ensure that the identity information

1. Ins. by Act 14 of 2019, sec. 8(a)(c) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
2. Ins. by Act 14 of 2019, sec. 8(a)(i) [w.e.f. 25-7-2019, vide S.O. 2649(F), dated 25th July, 2019].
3. Ins. by Act 14 of 2019, sec. 8(b) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
of an individual is only used for submission to the Central Identities Data Repository for authentication. It also provides that a requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication the details specified therein with respect to authentication. It further empowers the Authority to respond to an authentication query with a positive or negative response sharing such identity information excluding core biometric information.

(3A. Offline verification of Aadhaar number.—(1) Every offline verification of an Aadhaar number holder shall be performed in accordance with the provisions of this section.

(2) Every offline verification-seeking entity shall,—

(a) before performing offline verification, obtain the consent of an individual, or in the case of a child, his parent or guardian, in such manner as may be specified by regulations; and

(b) ensure that the demographic information or any other information collected from the individual for offline verification is only used for the purpose of such verification.

(3) An offline verification-seeking entity shall inform the individual undergoing offline verification, or in the case of a child, his parent or guardian the following details with respect to offline verification, in such manner as may be specified by regulations, namely:—

(a) the nature of information that may be shared upon offline verification;

(b) the uses to which the information received during offline verification may be put by the offline verification-seeking entity; and

(c) alternatives to submission of information requested for, if any.

(4) No offline verification-seeking entity shall—

(a) subject an Aadhaar number holder to authentication;

(b) collect, use, or store an Aadhaar number or biometric information of any individual for any purpose;

(c) take any action contrary to any obligation on it as may be specified by regulations.

9. Aadhaar number not evidence of citizenship or domicile, etc.—The Aadhaar number or the authentication thereof shall not, by itself, confer any right of, or be proof of, citizenship or domicile in respect of an Aadhaar number holder.

10. Central Identities Data Repository.—The Authority may engage one or more entities to establish and maintain the Central Identities Data Repository and to perform any other functions as may be specified by regulations.

CHAPTER IV

UNIQUE IDENTIFICATION AUTHORITY OF INDIA

11. Establishment of Authority.—(1) The Central Government shall, by notification, establish an Authority to be known as the Unique Identification Authority Of India to be responsible for the processes of enrollment and authentication and perform such other functions assigned to it under this Act.

(2) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of

1. Ins. by Act 14 of 2019, sec. 9 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 28th July, 2019].
this Act, to acquire, hold and dispose of property, both movable and immovable, 
and to contract, and shall, by the said name, sue or be sued. 
(3) The head office of the Authority shall be in New Delhi. 
(4) The Authority may, with the prior approval of the Central Government, 
establish its offices at other places in India.

NOTIFICATION

In exercise of the powers conferred by section 11 of the Aadhaar (Targeted Delivery 
of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), the Central 
Government, hereby establishes, the Unique Identification Authority of India, to exercise 
the powers conferred on, and to perform the functions assigned to it under the said Act, 
with effect from the date of publication of this notification in the Official Gazette.

2. The head office of the Authority shall be in New Delhi with regional offices 
at Bengaluru, Hyderabad, Lucknow, Guwahati, New Delhi, Ranchi, Mumbai and 
Chandigarh and offices for Central Identies Data Repository operations at Bengaluru and 
Mantaver.

[Vide S.O. 2358(III), dated 12th July, 2016, published in the Gazette of India, Extra., 
Pt. II, Sec. 3(iii), No. 1718, dated 12th July, 2016.]

12. Composition of Authority.—The Authority shall consist of a Chairperson, 
appointed on part-time or full-time basis, two part-time Members, and the 
Chief executive officer who shall be Member-Secretary of the Authority, to be 
appointed by the Central Government.

13. Qualifications for appointment of Chairperson and Members of 
Authority.—The Chairperson and Members of the Authority shall be persons 
of ability and integrity having experience and knowledge of at least ten years, 
in matters relating to technology, governance, law, development, economics, 
finance, management, public affairs or administration.

14. Term of office and other conditions of service of Chairperson and 
Members.—(1) The Chairperson and the Members appointed under this Act 
shall hold office for a term of three years from the date on which they assume 
office and shall be eligible for re-appointment:

Provided that no person shall hold office as the Chairperson or Member 
after he has attained the age of sixty-five years.

(2) The Chairperson and every Member shall, before entering office, make 
and subscribe to, an oath of office and of secrecy, in such form and in such 
manner and before such Authority as may be prescribed.

(3) Notwithstanding anything contained in sub-section (1), the Chairperson 
or Member may—
(a) relinquish his office, by giving in writing to the Central Government, 
a notice of not less than thirty days; or
(b) be removed from his office in accordance with the provisions of 
section 15.

(4) The salaries and allowances payable to, and the other terms and conditions 
of service of, the Chairperson and allowances or remuneration payable to part-
time Members shall be such as may be prescribed.

15. Removal of Chairperson and Members.—(1) The Central Government 
may remove from office, the Chairperson, or a Member, who—
(a) is, or at any time has been adjudged as insolvent;
(b) has become physically or mentally incapable of acting as the 
Chairperson or, as the case may be, a Member;
(c) has been convicted of an offence which, in the opinion of the Central 
Government, involves moral turpitude;
(d) has acquired such financial or other interest as is likely to affect prejudicially his functions as the Chairperson or, as the case may be, a Member; or

(e) has, in the opinion of the Central Government, so abused his position as to render his continuance in office detrimental to the public interest.

(2) The Chairperson or a Member shall not be removed under clause (b), clause (d) or clause (e) of sub-section (1) unless he has been given a reasonable opportunity of being heard.

16. Restrictions on Chairperson or Members on employment after cessation of office.—The Chairperson or a Member on ceasing to hold office for any reason, shall not, without previous approval of the Central Government,—

(a) accept any employment in, or be connected with the management of any organisation, company or any other entity which has been associated with any work done or contracted out by the Authority, whether directly or indirectly, during his tenure as Chairperson or Member, as the case may be, for a period of three years from the date on which he ceases to hold office:

Provided that nothing contained in this clause shall apply to any employment under the Central Government or a State Government or local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in clause (45) of section 2 of the Companies Act, 2013 (18 of 2013);

(b) act, for or on behalf of any person or organisation in connection with any specific proceeding or transaction or negotiation or a case to which the Authority is a party and with respect to which the Chairperson or such Member had, before cessation of office, acted for or provided advice to, the Authority;

(c) give advice to any person using information which was obtained in his capacity as the Chairperson or a Member and being unavailable to or not being able to be made available to the public; or

(d) enter, for a period of three years from his last day in office, into a contract of service with, accept an appointment to a board of directors of, or accept an offer of employment with, an entity with which he had direct and significant official dealings during his term of office.

COMMENTS

(Based on Notes on Clauses of the Bill)

This section prohibits as to holding of offices by the Chairperson or a Member on ceasing to be such Chairperson or a Member of the Authority. It provides that on ceasing to hold office, the Chairperson or Member of the Authority, as the case may be, shall subject to the provisions of the Act, be ineligible, for further employment in, or, connected with the management or administration of, any person which has been associated with any work under the Act, for a period of three years. It also provides that the section shall not apply to any employment under the Central Government or a State Government or
local authority or in any statutory authority or any corporation established by or under any Central, State or provincial Act or a Government Company, as defined in clause (45) of section 2 of the Companies Act, 2013 (18 of 2013).

17. **Functions of Chairperson.**—The Chairperson shall preside over the meetings of the Authority, and without prejudice to any provision of this Act, exercise and discharge such other powers and functions of the Authority as may be prescribed.

18. **Chief executive officer.—** (1) There shall be a chief executive officer of the Authority, not below the rank of Additional Secretary to the Government of India, to be appointed by the Central Government.

   (2) The chief executive officer shall be the legal representative of the Authority and shall be responsible for—
   
   (a) the day-to-day administration of the Authority;
   
   (b) implementing the work programmes and decisions adopted by the Authority;
   
   (c) drawing up of proposal for the Authority’s decisions and work programmes;
   
   (d) the preparation of the statement of revenue and expenditure and the execution of the budget of the Authority; and
   
   (e) performing such other functions, or exercising such other powers, as may be specified by regulations.

   (3) Every year, the chief executive officer shall submit to the Authority for approval—
   
   (a) a general report covering all the activities of the Authority in the previous year;
   
   (b) programmes of work;
   
   (c) the annual accounts for the previous year; and
   
   (d) the budget for the coming year.

   (4) The chief executive officer shall have administrative control over the officers and other employees of the Authority.

19. **Meetings of Authority.**—(1) The Authority shall meet at such times and places and shall observe such rules of procedure in regard to the transaction of business at its meetings, including quorum at such meetings, as may be specified by regulations.

   (2) The Chairperson, or, if for any reason, he is unable to attend a meeting of the Authority, the senior most Member shall preside over the meetings of the Authority.

   (3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes by the Members present and voting and in the event of an equality of votes, the Chairperson or in his absence the presiding Member shall have a casting vote.

   (4) All decisions of the Authority shall be signed by the Chairperson or any other Member or the Member-Secretary authorised by the Authority in this behalf.
(5) If any Member, who is a director of a company and who as such director, has any direct or indirect pecuniary interest in any manner coming up for consideration at a meeting of the Authority, he shall, as soon as possible after relevant circumstances have come to his knowledge, disclose the nature of his interest at such meeting and such disclosure shall be recorded in the proceedings of the Authority, and the Member shall not take part in any deliberation or decision of the Authority with respect to that matter.

20. Vacancies, etc, not to invalidate proceedings of Authority.—No act or proceeding of the Authority shall be invalid merely by reason of—
(a) any vacancy in, or any defect in the constitution of, the Authority;
(b) any defect in the appointment of a person as Chairperson or Member of the Authority; or
(c) any irregularity in the procedure of the Authority not affecting the merits of the case.

21. Officers and other employees of Authority.—(1) The Authority shall appoint such officers and employees as may be required for the discharge of its functions under this Act.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the officers and employees of the Authority shall be such as may be specified by regulations.

22. Transfer of assets, liabilities of Authority.—On and from the establishment of the Authority—
(a) all the assets and liabilities of 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, shall stand transferred to, and vested in, the Authority.

Explanation.—The assets of such Unique Identification Authority of India shall be deemed to include all rights and powers, and all properties, whether movable or immovable, including, in particular, cash balances, deposits and all other interests and rights in, or arising out of, such properties as may be in the possession of such Unique Identification Authority of India and all books of account and other documents relating to the same; and liabilities shall be deemed to include all debts, liabilities and obligations of whatever kind;

(b) without prejudice to the provisions of clause (a), all data and information collected during enrolment, all details of authentication performed, debts, obligations and liabilities incurred, all contracts entered into and all matters and things engaged to be done by, with or for such Unique Identification Authority of India immediately before that day, for or in connection with the purpose of the said Unique Identification Authority of India, shall stand transferred to, and vested in, the Authority.

1. Subs. by Act 14 of 2019, sec. 10, for section 21 [w.e.f. 25-7-2019], vide S.O. 2649(E), dated 25th July, 2019, Section 21, before substitution, stood as under:

21. Officers and other employees of Authority.—(1) The Authority may, with the approval of the Central Government, determine the number, nature and categories of other officers and employees required by the Authority in the discharge of its functions.

(2) The salaries and allowances payable to, and the other terms and conditions of service of, the chief executive officer and other officers and other employees of the Authority shall be such as may be specified by regulations with the approval of the Central Government."
Authority of India, shall be deemed to have been incurred, entered into or engaged to be done by, with or for, the Authority;

(c) all sums of money due to the said Unique Identification Authority of India immediately before that day shall be deemed to be due to the Authority; and

(d) all suits and other legal proceedings instituted or which could have been instituted by or against such Unique Identification Authority of India immediately before that day may be continued or may be instituted by or against the Authority.

23. Powers and functions of Authority.—(1) The Authority shall develop the policy, procedure and systems for issuing Aadhaar numbers to individuals and perform authentication thereof under this Act.

(2) Without prejudice to sub-section (1), the powers and functions of the Authority, inter alia, include—

(a) specifying, by regulations, demographic information and biometric information required for enrolment and the processes for collection and verification thereof;

(b) collecting demographic information and biometric information from any individual seeking an Aadhaar number in such manner as may be specified by regulations;

(c) appointing of one or more entities to operate the Central Identities Data Repository;

(d) generating and assigning Aadhaar numbers to individuals;

(e) performing authentication of Aadhaar numbers;

(f) maintaining and updating the information of individuals in the Central Identities Data Repository in such manner as may be specified by regulations;

(g) omitting and deactivating of an Aadhaar number and information relating thereto in such manner as may be specified by regulations;

(h) specifying the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used;

(i) specifying, by regulations, the terms and conditions for appointment of Registrars, enrolling agencies and service providers and revocation of appointments thereof;

(j) establishing, operating and maintaining of the Central Identities Data Repository;

(k) sharing, in such manner as may be specified by regulations, the information of Aadhaar number holders, subject to the provisions of this Act;

(l) calling for information and records, conducting inspections, inquiries and audit of the operations for the purposes of this Act of the Central Identities Data Repository, Registrars, enrolling agencies and other agencies appointed under this Act;

(m) specifying, by regulations, various processes relating to data management, security protocols and other technology safeguards under this Act;
(a) specifying, by regulations, the conditions and procedures for issuance of new Aadhaar number to existing Aadhaar number holder;

(b) levying and collecting the fees or authorising the Registrars, enrolling agencies or other service providers to collect such fees for the services provided by them under this Act in such manner as may be specified by regulations;

(c) appointing such committees as may be necessary to assist the Authority in discharge of its functions for the purposes of this Act;

(d) promoting research and development for advancement in biometrics and related areas, including usage of Aadhaar numbers through appropriate mechanisms;

(e) evolving of, and specifying by regulations, policies and practices for Registrars, enrolling agencies and other service providers;

(f) setting up facilitation centres and grievance redressal mechanism for redressal of grievances of individuals, Registrars, enrolling agencies and other service providers;

(g) such other powers and functions as may be prescribed.

(3) The Authority may,—

(a) enter into Memorandum of Understanding or agreement, as the case may be, with the Central Government or State Governments or Union territories or other agencies for the purpose of performing any of the functions in relation to collecting, storing, securing or processing of information or delivery of Aadhaar numbers to individuals or performing authentication;

(b) by notification, appoint such number of Registrars, engage and authorise such agencies to collect, store, secure, process information or do authentication or perform such other functions in relation thereto, as may be necessary for the purposes of this Act.

(4) The Authority may engage such consultants, advisors and other persons as may be required for efficient discharge of its functions under this Act on such allowances or remuneration and terms and conditions as may be specified by contract.

[23A. Power of Authority to issue directions.—(1) The Authority may for the discharge of its functions under this Act, or any rules or regulations made thereunder, by order, issue such directions from time to time to any entity in the Aadhaar ecosystem, as it may consider necessary.

(2) Every direction issued under sub-section (1) shall be complied with by the entity in the Aadhaar ecosystem to whom such direction is issued.]
25. Fund.—(1) There shall be constituted a Fund to be called the Unique Identification Authority of India Fund and there shall be credited thereto—
   (a) all grants, fees and charges received by the Authority under this Act; and
   (b) all sums received by the Authority from such other sources as may be decided upon by the Central Government.

(2) The Fund shall be applied for meeting—
   (a) the salaries and allowances payable to the Chairperson and members and administrative expenses including the salaries, allowances and pension payable to or in respect of officers and other employees of the Authority; and
   (b) the expenses on objects and for purposes authorised by this Act.

26. Accounts and audit.—(1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(2) The accounts of the Authority shall be audited annually by the Comptroller and Auditor-General of India at such intervals as may be specified by him and any expenditure incurred in connection with such audit shall be payable by the Authority to the Comptroller and Auditor-General.

(3) The Comptroller and Auditor-General of India and any person appointed by him in connection with the audit the accounts of the Authority under this Act shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General generally has in connection with the audit of Government accounts, and in particular, shall have the right to demand production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.

(4) The accounts of the Authority, as certified by the Comptroller and Auditor-General of India or any other person appointed by him in this behalf, together with the audit report thereon shall be forwarded annually to the Central Government by the Authority and the Central Government shall cause the audit report to be laid, as soon as may be after it is received, before each House of Parliament.

27. Returns and annual report, etc.—(1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and particulars in regard to any matter under the jurisdiction of the Authority, as the Central Government may from time to time require.

(2) The Authority shall prepare, once in every year, and in such form and manner and at such time as may be prescribed, an annual report giving—
   (a) a description of all the activities of the Authority for the previous years;
   (b) the annual accounts for the previous year; and

1. Sabs. by Act 14 of 2019, sec. 12, for section 25 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July 2019]. Section 25, before substitution, stood as under:
   "25. Other fees and revenues.—The fees or revenue collected by the Authority shall be credited to the Consolidated Fund of India."
(c) the programmes of work for coming year.

(3) A copy of the report received under sub-section (2) shall be laid by the Central Government, as soon as may be after it is received, before each House of Parliament.

CHAPTER VI
PROTECTION OF INFORMATION

28. Security and confidentiality of information.—(1) The Authority shall ensure the security of identity information and authentication records of individuals.

(2) Subject to the provisions of this Act, the Authority shall ensure confidentiality of identity information and authentication records of individuals.

(3) The Authority shall take all necessary measures to ensure that the information in the possession or control of the Authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under this Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.

(4) Without prejudice to sub-sections (1) and (2), the Authority shall—

(a) adopt and implement appropriate technical and organisational security measures;

(b) ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place appropriate technical and organisational security measures for the information; and

(c) ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority.

(5) Notwithstanding anything contained in any other law for the time being in force, and save as otherwise provided in this Act, the Authority or any of its officers, or other employees or any agency that maintains the Central Identities Data Repository shall not, whether during his service or thereafter, reveal any information stored in the Central Identities Data Repository or authentication record to anyone:

Provided that an Aadhaar number holder may request the Authority to provide access to his identity information excluding his core biometric information in such manner as may be specified by regulations.

29. Restriction on sharing information.—(1) No core biometric information, collected or created under this Act, shall be—

(a) shared with anyone for any reason whatsoever; or

(b) used for any purpose other than generation of Aadhaar numbers and authentication under this Act.

(2) The identity information, other than core biometric information, collected or created under this Act may be shared only in accordance with the provisions of this Act and in such manner as may be specified by regulations.
(3) No identity information available with a requesting entity or offline verification-seeking entity shall be—

(a) used for any purpose, other than the purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification; or

(b) disclosed for any purpose, other than purposes informed in writing to the individual at the time of submitting any information for authentication or offline verification:

Provided that the purposes under clauses (a) and (b) shall be in clear and precise language understandable to the individual.

(4) No Aadhaar number [demographic information or photograph] collected or created under this Act in respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.

COMMENTS

(Based on Notes on Clauses of the Bill)

This section provides for restriction on sharing information. It provides that identity information, other than core biometric information, collected or created under the Act may be shared only in accordance with the provisions of the Act and in such manner as may be specified by regulations.

30. Biometric information deemed to be sensitive personal information.— The biometric information collected and stored in electronic form, in accordance with this Act and regulations made thereunder, shall be deemed to be “electronic record” and “sensitive personal data or information”, and the provisions contained in the Information Technology Act, 2000 (21 of 2000) and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of this Act.

Explanation.—For the purposes of this section, the expressions—

(a) “electronic form” shall have the same meaning as assigned to it in clause (c) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000);

(b) “electronic record” shall have the same meaning as assigned to it in clause (c) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000);

(c) “sensitive personal data or information” shall have the same meaning as assigned to it in clause (iii) of the Explanation to section 43A of the Information Technology Act, 2000 (21 of 2000).

1. Subs. by Act 14 of 2019, sec. 13(a), for sub-section (3) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019]. Sub-section (3), before substitution, stood as under:

(3) No identity information available with a requesting entity shall be—

(a) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or

(b) disclosed further, except with the prior consent of the individual to whom such information relates.

2. Subs. by Act 14 of 2019, sec. 13(b), for “or core biometric information” [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
31. Alteration of demographic information or biometric information.—

(1) In case any demographic information of an Aadhaar number holder is found incorrect or changes subsequently, the Aadhaar number holder shall request the Authority to alter such demographic information in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(2) In case any biometric information of Aadhaar number holder is lost or changes subsequently for any reason, the Aadhaar number holder shall request the Authority to make necessary alteration in his record in the Central Identities Data Repository in such manner as may be specified by regulations.

(3) On receipt of any request under sub-section (1) or sub-section (2), the Authority may, if it is satisfied, make such alteration as may be required in the record relating to such Aadhaar number holder and intimate such alteration to the concerned Aadhaar number holder.

(4) No identity information in the Central Identities Data Repository shall be altered except in the manner provided in this Act or regulations made in this behalf.

32. Access to own information and records of requests for authentication.—

(1) The Authority shall maintain authentication records in such manner and for such period as may be specified by regulations.

(2) Every Aadhaar number holder shall be entitled to obtain his authentication record in such manner as may be specified by regulations.

(3) The Authority shall not, either by itself or through any entity under its control, collect, keep or maintain any information about the purpose of authentication.

33. Disclosure of information in certain cases.—(1) Nothing contained in sub-section (2) or sub-section (5) of section 28 or sub-section (2) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made pursuant to an order of a court not inferior to that of a Judge of a High Court:

Provided that no order by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority [and the concerned Aadhaar number holder]:

[Provided further that the core biometric information shall not be disclosed under this sub-section.]

(2) Nothing contained in sub-section (2) or sub-section (5) of section 28 and clause (b) of sub-section (1), sub-section (2) or sub-section (3) of section 29 shall apply in respect of any disclosure of information, including identity information or authentication records, made in the interest of national security in pursuance of a direction of an officer not below the rank of [Secretary] to the Government of India specially authorised in this behalf by an order of the Central Government:

1. Subs. by Act 14 of 2019, sec. 140(c), for “District Judge” [w.e.f. 25-7-2019, vide S.O. 2648(E), dated 25th July, 2019].
2. Ins. by Act 14 of 2019, sec. 140(b) [w.e.f. 25-7-2019, vide S.O. 2648(E), dated 25th July, 2019].
3. Ins. by Act 14 of 2019, sec. 140(b) [w.e.f. 25-7-2019, vide S.O. 2648(E), dated 25th July, 2019].
4. Subs. by Act 14 of 2019, sec. 140(b), for “Joint Secretary” [w.e.f. 25-7-2019, vide S.O. 2640(E), dated 25th July, 2019].
Provided that every direction issued under this sub-section, shall be reviewed by an Oversight Committee consisting of the Cabinet Secretary and the Secretaries to the Government of India in the Department of Legal Affairs and the Department of Electronics and Information Technology, before it takes effect.

Provided further that any direction issued under this sub-section shall be valid for a period of three months from the date of its issue, which may be extended for a further period of three months after the review by the Oversight Committee.

1[CHAPTER VIA

CIVIL PENALTIES

33A. Penalty for failure to comply with provisions of this Act, rules, regulations and directions.—(1) Where an entity in the Aadhaar ecosystem fails to comply with the provision of this Act, the rules or regulations made thereunder or directions issued by the Authority under section 23A, or fails to furnish any information, document, or return of report required by the Authority, such entity shall be liable to a civil penalty which may extend to one crore rupees for each contravention and in case of a continuing failure, with additional penalty which may extend to ten lakh rupees for every day during which the failure continues after the first contravention.

(2) The amount of any penalty imposed under this section, if not paid, may be recovered as if it were an arrear of land revenue.

33B. Power to adjudicate.—(1) For the purposes of adjudication under section 33A and imposing a penalty thereunder, the Authority shall appoint an officer of the Authority, who is not below the rank of a Joint Secretary to the Government of India and possessing such qualification and experience as may be prescribed, to be an Adjudicating Officer for holding an inquiry in such manner as may be prescribed.

(2) No inquiry under sub-section (1) shall be initiated except by a complaint made by the Authority.

(3) While holding an inquiry, the Adjudicating Officer shall—

(a) provide the entity in the Aadhaar ecosystem against whom complaint is made, an opportunity of being heard;

(b) have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

(4) If the Adjudicating Officer, on such inquiry, is satisfied that the entity in the Aadhaar ecosystem has failed to comply with any provision of this Act or the rules or regulations made thereunder or directions issued by the Authority under section 23A, or has failed to furnish any information, document, or return

1. Chapter VIA (containing sections 33A to 33F) ins. by Act 14 of 2019, sec. 15 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
of report required by the Authority, the Adjudicating Officer may, by order, impose such penalty under section 33A as he thinks fit.

33C. Appeals to Appellate Tribunal.—(1) The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997), shall be the Appellate Tribunal for the purposes of hearing appeals against the decision of the Adjudicating Officer under this Act.

(2) A person or entity in the Aadhaar ecosystem aggrieved by an order of the Adjudicating Officer under section 30B, may prefer an appeal to the Appellate Tribunal within a period of forty-five days from the date of receipt of the order appealed against, in such form and manner and accompanied with such fee as may be prescribed:

Provided that the Appellate Tribunal may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.

(3) On receipt of an appeal under sub-section (2), the Appellate Tribunal may, after giving the parties to the appeal an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(4) The Appellate Tribunal shall send a copy of every order made by it to the parties to the appeal and to the Adjudicating Officer.

(5) Any appeal filed under sub-section (2) shall be dealt with by the Appellate Tribunal as expeditiously as possible and every endeavour shall be made by it to dispose of the appeal within six months from the date on which it is presented to it.

(6) The Appellate Tribunal may, for the purpose of deciding an appeal before it, call for the records relevant to disposing of such appeal and make such orders as it thinks fit.

33D. Procedure and powers of the Appellate Tribunal.—The provisions of sections 14-D to 14K (both inclusive), 16 and 17 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) shall, mutatis mutandis, apply to the Appellate Tribunal in the discharge of its functions under this Act, as they apply to it in the discharge of its functions under that Act.

33E. Appeal to Supreme Court of India.—(1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law for the time being in force, an appeal shall lie against any order, not being an interlocutory order, of the Appellate Tribunal, to the Supreme Court on any substantial question of law arising out of such order.

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal which the parties have consented to.

(3) Every appeal under this section shall be preferred within a period of forty-five days from the date of the decision or order appealed against:

Provided that the Supreme Court may entertain an appeal after the expiry of the said period of forty-five days if it is satisfied that there was sufficient cause for not filing it within that period.
CHAPTER VII
OFFENCES AND PENALTIES

34. Penalty for impersonation at time of enrolment.—Whoever impersonates or attempts to impersonate another person, whether dead or alive, real or imaginary, by providing any false demographic information or biometric information, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or with both.

35. Penalty for impersonation of Aadhaar number holder by changing demographic information or biometric information.—Whoever, with the intention of causing harm or mischief to an Aadhaar number holder, or with the intention of appropriating the identity of an Aadhaar number holder changes or attempts to change any demographic information or biometric information of an Aadhaar number holder by impersonating or attempting to impersonate another person, dead or alive, real or imaginary, shall be punishable with imprisonment for a term which may extend to three years and shall also be liable to a fine which may extend to ten thousand rupees.

36. Penalty for impersonation.—Whoever, not being authorised to collect identity information under the provisions of this Act, by words, conduct or demeanour pretends that he is authorised to do so, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

37. Penalty for disclosing identity information.—Whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised under this Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of this Act, shall be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

COMMENTS
(Based on Notes on Clauses of the Bill)

This section provides for penalty for disclosing identity information. It provides that whoever, intentionally discloses, transmits, copies or otherwise disseminates any identity information collected in the course of enrolment or authentication to any person not authorised under the Act or regulations made thereunder or in contravention of any agreement or arrangement entered into pursuant to the provisions of the Act, shall be
punishable with imprisonment for a term which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

38. Penalty for unauthorised access to the Central Identities Data Repository.—Whoever, not being authorised by the Authority, intentionally,—
(a) accesses or secures access to the Central Identities Data Repository;
(b) downloads, copies or extracts any data from the Central Identities Data Repository or stored in any removable storage medium;
(c) introduces or causes to be introduced any virus or other computer contaminant in the Central Identities Data Repository;
(d) damages or causes to be damaged the data in the Central Identities Data Repository;
(e) disrupts or causes disruption of the access to the Central Identities Data Repository;
(f) denies or causes a denial of access to any person who is authorised to access the Central Identities Data Repository;
(g) reveals any information in contravention of sub-section (5) of section 28, or shares, uses or displays information in contravention of section 29 or assists any person in any of the aforementioned acts;
(h) destroys, deletes or alters any information stored in any removable storage media or in the Central Identities Data Repository or diminishes its value or utility or affects it injuriously by any means; or
(i) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used by the Authority with an intention to cause damage,
shall be punishable with imprisonment for a term which may extend to 3 years and shall also be liable to a fine which shall not be less than ten thousand rupees.

Explanations.—For the purposes of this section, the expressions "computer contaminant", "computer virus" and "damage" shall have the meanings respectively assigned to them in the Explanation to section 43 of the Information Technology Act, 2000 (21 of 2000), and the expression "computer source code" shall have the meaning assigned to it in the Explanation to section 63 of the said Act.

39. Penalty for tampering with data in Central Identities Data Repository.—Whoever, not being authorised by the Authority, uses or tampers with the data in the Central Identities Data Repository or in any removable storage medium with the intent of modifying information relating to Aadhaar number holder or discovering any information thereof, shall be punishable with imprisonment for a term which may extend to 3 years and shall also be liable to a fine which may extend to ten thousand rupees.

1. Subs. by Act 14 of 2019, sec. 16, for "three years" [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
2. Subs. by Act 14 of 2019, sec. 17, for "three years" [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
40. Penalty for unauthorised use by requesting entity or offline verification seeking entity.—Whoever,—

(a) being a requesting entity, uses the identity information of an individual in contravention of sub-section (2) of section 8; or

(b) being an offline verification-seeking entity, uses the identity information of an individual in contravention of sub-section (2) of section 8A,

shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

41. Penalty for non-compliance with intimation requirements.—Whoever, being an enrolling agency or a requesting entity, fails to comply with the requirements of sub-section (2) of section 3 or sub-section (3) of section 8, shall be punishable with imprisonment which may extend to one year or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.

42. General penalty.—Whoever commits an offence under this Act or any rules or regulations made thereunder for which no specific penalty is provided elsewhere than this section, shall be punishable with imprisonment for a term which may extend to [three years] or with a fine which may extend to twenty-five thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees, or with both.

43. Offences by companies.—(1) Where an offence under this Act has been committed by a company, every person who at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment provided in this Act if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

(2) Notwithstanding anything contained in sub-section (1), where any offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to, any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be

1. Subs. by Act 14 of 2019, sec. 16, for section 40 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019]. Section 40, before substitution, stood as under:

"40. Penalty for unauthorised use by requesting entity.—Whoever, being a requesting entity, uses the identity information of an individual in contravention of sub-section (3) of section 8, shall be punishable with imprisonment which may extend to three years or with a fine which may extend to ten thousand rupees or, in the case of a company, with a fine which may extend to one lakh rupees or with both.".

2. Subs. by Act 14 of 2019, sec. 19, for "one year" [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation.—For the purposes of this section—
(a) “company” means any body corporate and includes a firm or other association of individuals; and
(b) “director”, in relation to a firm, means a partner in the firm.

44. Act to apply for offence or contravention committed outside India.—(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person, irrespective of his nationality.

(2) For the purposes of sub-section (1), the provisions of this Act shall apply to any offence or contravention committed outside India by any person, if the act or conduct constituting the offence or contravention involves any data in the Central Identities Data Repository.

45. Power to investigate offences.—Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector of Police shall investigate any offence under this Act.

46. Penalties not to interfere with other punishments.—No penalty imposed under this Act shall prevent the imposition of any other penalty or punishment under any other law for the time being in force.

47. Cognizance of offences.—(1) No court shall take cognizance of any offence punishable under this Act, save on a complaint made by the Authority or any officer or person authorised by it:

[Provided that the court may, on a complaint made by an Aadhaar number holder or individual take cognizance of any offence punishable under section 34 or 35 or 36 or 37 or 40 or section 41.]

(2) No court inferior to that of a Chief Metropolitan Magistrate or a Chief Judicial Magistrate shall try any offence punishable under this Act.

CHAPTER VIII
MISCELLANEOUS

48. Power of Central Government to supersede Authority.—(1) If, at any time, the Central Government is of the opinion,—

(a) that, on account of circumstances beyond the control of the Authority, it is unable to discharge the functions or perform the duties imposed on it by or under the provisions of this Act; or

(b) that the Authority has persistently defaulted in complying with any direction given by the Central Government under this Act or in the discharge of the functions or performance of the duties imposed on it by or under the provisions of this Act and as a result of such default the financial position of the Authority or the administration of the Authority has suffered; or

(c) that a public emergency exists,

1. Ins. by Act 14 of 2019, sec. 20 (w.e.f. 25-7-2019; vide S.O. 2649(E), dated 25th July, 2019).
the Central Government may, by notification, supersede the Authority for such period, not exceeding six months, as may be specified in the notification and appoint a person or persons as the President may direct to exercise powers and discharge functions under this Act:

Provided that before issuing any such notification, the Central Government shall give a reasonable opportunity to the Authority to make representations against the proposed supersession and shall consider the representations, if any, of the Authority.

(2) Upon the publication of a notification under sub-section (1), superseding the Authority,—

(a) the Chairperson and other Members shall, as from the date of supersession, vacate their offices as such;

(b) all the powers, functions and duties which may, by or under the provisions of this Act, be exercised or discharged by or on behalf of the Authority shall, until the Authority is reconstituted under sub-section (3), be exercised and discharged by the person or persons referred to in sub-section (1); and

(c) all properties owned or controlled by the Authority shall, until the Authority is reconstituted under sub-section (3), vest in the Central Government.

(3) On or before the expiration of the period of supersession specified in the notification issued under sub-section (1), the Central Government shall reconstitute the Authority by a fresh appointment of its Chairperson and other Members and in such case any person who had vacated his office under clause (a) of sub-section (2) shall not be deemed to be disqualified for reappointment.

(4) The Central Government shall cause a copy of the notification issued under sub-section (1) and a full report of any action taken under this section and the circumstances leading to such action to be laid before each House of Parliament at the earliest.

49. Members, officers, etc., to be public servants.—The Chairperson, Members, officers and other employees of the Authority shall be deemed, while acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code (45 of 1860).

50. Power of Central Government to issue directions.—(1) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act be bound by such directions on questions of policy, as the Central Government may give, in writing to it, from time to time:

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section:
Provided further that nothing in this section shall empower the Central Government to issue directions pertaining to technical or administrative matters undertaken by the Authority.

(2) The decision of the Central Government, whether a question is one of policy or not, shall be final.

50A. Exemption from tax on income.—Notwithstanding anything contained in the Income Tax Act, 1961 (43 of 1961) or any other enactment for the time being in force relating to tax on income, profits or gains, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains.

51. Delegation.—The Authority may, by general or special order in writing, delegate to any [Member or officer] of the Authority or any other person, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act (except the power under section 54) as it may deem necessary.

52. Protection of action taken in good faith.—No suit, prosecution or other legal proceeding shall lie against the Central Government or the Authority or the Chairperson or any Member or any officer, or other employees of the Authority for anything which is in good faith done or intended to be done under this Act or the rule or regulation made thereunder.

53. Power of Central Government to make rules.—(1) The Central Government may, by notification, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely—

(a) the form and manner in which and the authority before whom the oath of office and of secrecy is to be subscribed by the Chairperson and Members under sub-section (2) of section 14;

(b) the purpose for which the requesting entity may be allowed by the Authority to perform authentication under sub-clause (ii) of clause (b) of sub-section (4) of section 4;

(c) the salary and allowances payable to, and other terms and conditions of service of, the Chairperson and the allowances or remuneration payable to Members of the Authority under sub-section (4) of section 14;

(d) the other powers and functions of the Chairperson of the Authority under section 17;

(e) the other powers and functions of the Authority under clause (c) of sub-section (2) of section 23;

(f) the form of annual statement of accounts to be prepared by Authority under sub-section (1) of section 26;

1. Ins. by Act 14 of 2019, sec. 21 [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
2. Subs. by Act 14 of 2019, sec. 22, for “Member, officer” [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
3. Ins. by Act 14 of 2019, sec. 23(I) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
(f) the form and the manner in which and the time within which returns and statements and particulars are to be furnished under sub-section (1) of section 27;

(g) the form and the manner and the time at which the Authority shall furnish annual report under sub-section (2) of section 27;

1[(ga) the qualification and experience of, and the manner of appointment of, the Adjudicating Officer under sub-section (1) of section 33B;]

1[(gb) the form, manner, and fee for an appeal to be filed under sub-section (2) of section 33C;]

(h) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be or may be made by rules.

54. Power of Authority to make regulations.—(1) The Authority may, by notification, make regulations consistent with this Act and the rules made thereunder, for carrying out the provisions of this Act:

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:—

2[(a) the entities or group of entities in the Aadhaar ecosystem under clause (aa), the biometric information under clause (g) and the demographic information under clause (k), the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (m), and the modes of offline verification of Aadhaar number holder under clause (pa) of section 2;]

(b) the manner of verifying the demographic information and biometric information for issue of Aadhaar number under sub-section (3) of section 3;

3[(ba) the manner of generating an alternative virtual identity under sub-section (4) of section 3;]

3[(bb) the manner in which cancellation of an Aadhaar number may be carried out under sub-section (2) of section 3A;]

(c) the conditions for accepting an Aadhaar number as proof of identity of the Aadhaar number holder under sub-section (3) of section 4;

4[(ca) standards of privacy and security to be complied with by the requesting entities under sub-section (4) of section 4;]

4[(cb) the classification of requesting entities under sub-section (5) of section 4;]

1. Ins. by Act 14 of 2019, sec. 23(ii) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
2. Subs. by Act 14 of 2019, sec. 24(0), for clause (a) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019]. Clause (a), before substitution, stood as under:

“(a) the biometric information under clause (g) and the demographic information under clause (k), and the process of collecting demographic information and biometric information from the individuals by enrolling agencies under clause (m) of section 2”;

3. Ins. by Act 14 of 2019, sec. 24(ii) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
4. Ins. by Act 14 of 2019, sec. 24(iii) [w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019].
(d) the other categories of individuals under section 5 for whom the Authority shall take special measures for allotment of Aadhaar number;

(e) the manner of updating biometric information and demographic information under section 6;

(f) the procedure for authentication of the Aadhaar number under section 8;

1[(fa) the alternate and viable means of identification of individual under the proviso to clause (b) of sub-section (2) of section 8;]

1[(fb) the manner of obtaining consent under clause (a) of sub-section (2), the manner of providing information to the individual undergoing offline verification under sub-section (3), and the obligations of offline verification-seeking entities under clause (c) of sub-section (4), of section 8A;]

(g) the other functions to be performed by the Central Identities Data Repository under section 10;

(h) the time and places of meetings of the Authority and the procedure for transaction of business to be followed by it, including the quorum, under sub-section (1) of section 19;

(i) the salary and allowances payable to, and other terms and conditions of service of, the chief executive officer, officers and other employees of the Authority under sub-section (2) of section 21;

(j) the demographic information and biometric information under clause (a) and the manner of their collection under clause (b) of sub-section (2) of section 23;

(k) the manner of maintaining and updating the information of individuals in the Central Identities Data Repository under clause (f) of sub-section (2) of section 23;

(l) the manner of omitting and deactivating an Aadhaar number and information relating thereto under clause (g) of sub-section (2) of section 23;

(m) the manner of use of Aadhaar numbers for the purposes of providing or availing of various subsidies, benefits, services and other purposes for which Aadhaar numbers may be used under clause (h) of sub-section (2) of section 23;

(n) the terms and conditions for appointment of Registrars, enrolling agencies and other service providers and the revocation of appointments thereof under clause (i) of sub-section (2) of section 23;

(o) the manner of sharing information of Aadhaar number holder under clause (k) of sub-section (2) of section 23;

(p) various processes relating to data management, security protocol and other technology safeguards under clause (m) of sub-section (2) of section 23;

1. Ins. by Act 14 of 2019, sec. 24(iv) [w.e.f. 25-7-2019,vide S.O. 2649(E), dated 29th July, 2019].
The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016

(q) the procedure for issuance of new Aadhaar number to existing Aadhaar number holder under clause (a) of sub-section (2) of section 23;

(r) manner of authorising Registrars, enrolling agencies or other service providers to collect such fees for services provided by them under clause (o) of sub-section (2) of section 23;

(s) policies and practices to be followed by the Registrar, enrolling agencies and other service providers under clause (r) of sub-section (2) of section 23;

(t) the manner of accessing the identity information by the Aadhaar number holder under the proviso to sub-section (5) of section 28;

(u) the manner of sharing the identity information, other than core biometric information, collected or created under this Act under sub-section (2) of section 29;

(v) the manner of alteration of demographic information under sub-section (1) and biometric information under sub-section (2) of section 31;

(w) the manner of and the time for maintaining the request for authentication and the response thereon under sub-section (1), and the manner of obtaining, by the Aadhaar number holder, the authentication records under sub-section (2) of section 32;

(x) any other matter which is required to be, or may be, specified, or in respect of which provision is to be or may be made by regulations.

55. Laying of rules and regulations before Parliament.—Every rule and every regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation, or both the Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

56. Application of other laws not barred.—The provisions of this Act shall be in addition to, and not in derogation of, any other law for the time being in force.

1[57. Act not to prevent use of Aadhaar number for other purposes under law.—Repealed by the Aadhaar and other Laws (Amendment) Act, 2019 (14 of 2019), sec 25 (w.e.f. 25-7-2019, vide S.O. 2649(E), dated 25th July, 2019).]]

---

1. Section 57, before omission, stood as under:

"57. Act not to prevent use of Aadhaar number for other purposes under law.—Nothing contained in this Act shall prevent the use of Aadhaar number for establishing the identity of an individual for any purpose, whether by the State or any body corporate or person, pursuant to any law, for the time being in force, or any contract to this effect:

Provided that the use of Aadhaar number under this section shall be subject to the procedure and obligations under section 8 and Chapter VI."
58. Power to remove difficulties.—(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of three years from the commencement of this Act.

(2) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

59. Savings.—Anything done or any action taken by the Central Government under the Resolution of the Government of India, Planning Commission bearing notification number A-43011/92/2009- Admin. I, dated the 28th January, 2009, or by the Department of Electronics and Information Technology under the Cabinet Secretariat Notification bearing notification number S.O. 2492(E), dated the 12th September, 2015, as the case may be, shall be deemed to have been validly done or taken under this Act.
THE AADHAAR (REMOVAL OF DIFFICULTIES) ORDER, 2016

WHEREAS, the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016 (the said Act) received the assent of the President on 25th March 2016 and was published in the Gazette of India on 26th March 2016;

AND WHEREAS, sections 11 to 20, 22 to 23 and sections 48 to 59 have come into force and the Unique Identification Authority of India (the Authority) has been established under section 12 of the Act on 12th July 2016;

AND WHEREAS, the Unique Identification Authority of India (Terms and Conditions of Service of Chairperson and Members) Rules, 2016 have been notified on 12th July 2016 which require selection of the Chairperson and members through a Search-cum-Selection Committee headed by the Cabinet Secretary;

AND WHEREAS, only after completion of the selection process, the Chairperson and members can be appointed under section 12 of the Act and various regulations which are required to give effect to the provisions of the Act can be framed by the Authority, which is likely to take some time;

AND WHEREAS, till such time that the Chairperson and Members are appointed and regulations framed, difficulties may arise in the Authority discharging its powers and functions under section 23 without having in place the regulations necessary for the same, which may result in residents being unable to receive subsides, benefits, and services by using the Aadhaar number;

NOW, THEREFORE, in exercise of the powers conferred by sub-section (1) of section 58(1) of the said Act, the Central Government hereby makes the following Order to remove the aforesaid difficulties, namely:

1. Short title and commencement.—(1) This Order may be called the Aadhaar (Removal of Difficulties) Order, 2016.

   (2) It shall be deemed to have come into force from the 12th of July, 2016, and shall be in force till such time all provisions of the Act come into force and regulations are made which are necessary to give effect to the said provisions, or till the expiry of three months from the date on which this order comes into force, whichever is earlier.

2. Continuance of procedures to be followed by the Authority.—(1) The procedures, processes, practices, guidelines, and circulars issued by the Unique Identification Authority of India established vide Resolution of the Government of India, Planning Commission bearing notification number A-43611/02/2009-Admin. I, dated the 28th January, 2009, or issued under the Cabinet Secretariat Notification bearing notification number S.O. 2492(E), dated the 12th September, 2015 shall continue to be followed by the Authority established under section 11 of the said Act till such time this Order is in force:

Provided that till such time this Order is in force, the processes of enrolment shall continue and consents shall be obtained as per the provisions contained in sub-section 2 of section 3 of the said Act in revised sample forms, incorporating the new formats for consent as given in Schedule 1A and 1B.

(2) All actions that may be taken by the Central Government, the Authority, their officers, and staff in accordance with the said procedures, processes, policies, practices and systems shall be deemed to be actions authorised under this Act.

SCHEDULE 1A
AADHAAR ENROLMENT/CORRECTION FORM

SCHEDULE 1B
AADHAAR DATA UPDATE/CORRECTION FORM

For Forms please visit website of Unique Identification Authority of India (www.uidai.gov.in)
THE UNIQUE IDENTIFICATION AUTHORITY
OF INDIA (TRANSACTION OF BUSINESS
AT MEETINGS OF THE AUTHORITY)
REGULATIONS, 2016

In exercise of the powers conferred by clause (h) of sub-section (2) of section 54 read
with sub-section (1) of section 19 of the Aadhaar (Targeted Delivery of Financial and
other Subsidies, Benefits and Services) Act, 2016 (18 of 2016), the Unique Identification
Authority of India hereby makes the following regulations regulating the transaction of
business in the meetings of the Unique Identification Authority of India, namely:—

1. Short title and commencement.—(1) These regulations may be called the
Unique Identification Authority of India (Transaction of Business at Meetings of
the Authority) Regulations, 2016.

(2) They shall come into force on the date\textsuperscript{2} 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 (18 of 2016);

(b) “Authority” means the Unique Identification Authority of India
established under sub-section (1) of section 11 of the Act;

(c) “Chairperson” means the Chairperson of the Authority appointed
under section 12 of the Act;

(d) “Member” includes the Chairperson and Member of the Authority
appointed under section 12;

(e) “Chief Executive Officer” means the Chief Executive Officer, who
shall be Member Secretary of the Authority, appointed under sub-
section (1) of section 18 of the Act;

(f) “Meeting” means meeting convened by the Authority as per sub-
section (1) of section 19 of the Act;

(g) “Schedule” means a Schedule appended to these regulations.

(2) Words and expressions used herein but not defined, and defined in the
Act, shall have the same meanings assigned to them in the Act.

3. Meetings of the Authority.—(1) There shall be no less than three meetings
of the Authority in a financial year on such dates and at such places as the
Chairperson may direct and the interval between any two meetings shall not
in any case, be longer than five months:

Provided that the first meeting of the Authority in a financial year shall be
held in the first quarter of that financial year.

\textsuperscript{1} Vide Notification No. 12012/64/2016/Legal/UIDAI (No. 1 of 2016), dated 12th
September, 2016, published in the Gazette of India, Extra., Pt. III, Sec. 4, No. 347, dated 14th
September, 2016.

\textsuperscript{2} Came into force on 14-9-2016.
(2) The notice of every meeting of the Authority shall be signed by the Chief Executive Officer intimating the time, date and place of the intended meeting.

(3) The notice shall be given to every member, at least 15 days before the date of the meeting by post to the address of every member or through e-mail or courier or Fax to facilitate speedy communication, stating therein the brief agenda of the meeting, setting out the items of business to be considered.

(4) The Chairperson, may, in case of urgency, at any time, call a meeting of the Authority at a lesser notice than fifteen days.

(5) A meeting of the Authority may be called on the requisition in writing, addressed to the Chairperson, and signed by the Chief Executive Officer or signed by not less than half of the members, setting out therein the purpose of the meeting to be called and the business to be considered thereat.

(6) On receipt of the requisition of meeting, the Chairperson may direct to cause the meeting to be convened and held within such time as he may direct, but in any case not later than a period of 15 days from the date of receipt of such requisition.

(7) If all the items of business to be transacted at a meeting of the Authority cannot be completed in one sitting, the meeting may be adjourned from time to time:

Provided that at the meeting convened post adjournment only the unfinished items in the Agenda shall be discussed and decision taken thereon.

4. Chairperson of the meetings of the Authority.—(1) The Chairperson shall preside over the meetings of the Authority. In his absence, the senior most among the Members and Member Secretary, in terms of date of appointment to the Authority, shall preside over the meetings of the Authority.

(2) The Chairperson of the meeting may also invite any officer of the Authority or any other person qualified in the matters to be discussed at any meeting to attend any meeting of the Authority, with a view to facilitate meaningful discussions and such invitee may participate in the proceedings of the meeting but shall have no right to vote.

5. Participation of the Chief Executive Officer.—(1) The Chief Executive Officer shall participate in meeting of the Authority as Member Secretary of the Authority.

(2) The Chief Executive Officer may, with permission of Chairperson, take the assistance of any staff of the Authority for the purpose of discharging his duties relating to the meetings of the Authority.

6. Quorum.—(1) The quorum for any meeting of the Authority shall be two and no business shall be transacted at any meeting of the Authority unless the quorum is present throughout the meeting.

(2) If the quorum is not present at any meeting of the Authority, the Chairperson or in his absence, the Chief Executive Officer or the senior most Member presiding over the meeting, shall adjourn the meeting to such other date, time and place as may be specified by him not being later than thirty days:
Provided that if at such adjourned meeting quorum is not present, then, notwithstanding anything contained in sub-regulation (1), the Members present at the said adjourned meeting, shall constitute a quorum for such meeting to take up discussion and to dispose of only the items of business set out in the agenda for the initial meeting.

7. Agenda.—(1) The Chief Executive Officer shall be responsible for preparation of the agenda for each meeting of the Authority and circulation thereof to all the Members of the Authority at least a period of seven days before the date of each meeting:

Provided that the Chief Executive Officer shall prepare the agenda of meeting in consultation with the Chairperson:

Provided further that Chief Executive Officer may, in consultation with the Chairperson, amend or delete or add new item in the Agenda of business subsequent to its issue.

(2) Any business not included in the agenda shall not be transacted at a meeting of the Authority except with the permission of the Chairperson or other Member presiding over the meeting.

(3) With the permission of the Chairperson or other Member presiding over the meeting, urgent questions may be added to the Agenda at any time before the conclusion of the meeting, or any item on the Agenda may be deleted or carried over to a subsequent meeting.

8. Decision of meetings of the Authority.—(1) If a Member has an interest in any item of business to be transacted at a meeting, he shall not participate or vote on such item and in such case, the decision on such item shall be taken by majority of the votes of other Members attending the meeting.

(2) The Chairperson or the other Member presiding over the meeting shall endeavour at all times to arrive at decisions or recommendations through a consensus among Members and voting shall be resorted to if attempts to arrive at a consensus fail. In the event of equality of votes, the Chairperson, or, in his absence, the presiding Member, shall have a casting vote.

(3) Votes on every item of business to be transacted at a meeting of the Authority shall be taken by a show of hands.

(4) All decisions of the Authority shall be signed by the Member-Secretary of the Authority.

(5) Decisions taken at every meeting of the Authority shall be published on the website of Authority unless the Chairperson determines otherwise on grounds of ensuring confidentiality.

9. Closure of debates.—(1) The Chairperson or the Member presiding over the meeting may move for the closure of the debate or any item of business discussed at a meeting when he considers that all members have had the opportunity to express their views on any business discussed at the meeting and the decision of the Chairperson or the Member presiding shall be final.

10. Minutes of meeting of the Authority.—(1) The Chief Executive Officer shall cause the draft minutes of each meeting of the Authority to be prepared
within a period of two weeks of conclusion of each meeting and submit the
same to the Chairperson or other Member who presided over the meeting, for
his approval:

Provided that if for any reasons the Chief Executive Officer is unable to
attend any meeting of the Authority, the Chairperson may, for this temporary
purpose direct any other officer of the Authority, to prepare minutes of the
meeting.

(2) The draft minutes of each meeting of the Authority approved by the
Chairperson or the other Member who presided over that meeting shall be
forwarded to each member not later than a period of two weeks from such
approval, for adoption at the next meeting:

Provided that the decision of the Chairperson on the changes, if any, to be
made in the draft minutes, shall be final.

(3) The minutes of each meeting of the Authority shall contain a fair and
correct summary of the proceedings thereat and the names of Members who did
not participate in the discussion of, or vote on, any item of business transacted
at the meeting.

(4) The Chairperson or other Member who presided over the meeting may
decide the inclusion or non-inclusion of any matter in the minutes, if in his
opinion, the same is not relevant or material to the proceedings or defamatory
of any person.

(5) At every meeting of the Authority, the draft minutes of the previous
meeting approved by the Chairperson or the other Member who presided over
that previous meeting shall be placed before the meeting for confirmation and
adoption, with or without amendments or modifications, and upon confirmation
and adoption in that meeting, be signed by the Chairperson or other Member
presiding over the meeting, as confirmation of correctness of the record of the
proceedings of the previous meeting and be kept as a record of the Authority.

11. Power of the Chief Executive Officer to take urgent action.—The
Chief Executive Officer may take such action as may be necessary in case of an
emergency situation warranting immediate action by the Authority and when it
is not feasible to call a meeting of the Authority, and for the reasons be recorded
in writing:

Provided that any such action or decision, as the case may be, shall be
communicated to all the Members within a period of seven days:

Provided further that any such action shall be placed in the next meeting
of the Authority for its ratification.

12. Decision by circulation.—(1) Any item of business or issue which
requires decision of the Authority, if the Chairperson so directs, may be referred
to Members by circulation of the matter as a resolution.

(2) A resolution shall be deemed to have been passed by the Members when
such a resolution circulated in the draft, together with necessary material, if any,
to all the Members to their official e-mail ids and the resolution is approved by
the majority of the Members:
Provided that the replies of all Members shall be obtained within a period not more than three clear days.

(3) Any resolution circulated under sub-regulation (1) and approved by the majority of such of those Members entitled to vote thereon, shall have such effect and be binding as if such resolution were decided by the majority of the members at a meeting.

(4) Based upon the votes and comments received on the draft resolution circulated under sub-regulation (1), the Chairperson may—
   (a) declare the decision adopted; or
   (b) declare the decision not adopted; or
   (c) in case of neutrality of votes, postpone draft resolution for the next meeting of the Authority.

(5) Any resolution passed through circulation, shall be placed at the next meeting of the Authority for its ratification.

13. Record of Business.—(1) The Chief Executive Officer shall attend the meetings of the Authority, maintain the record of proceedings of all items of the business transacted thereat.

(2) Every decision and direction of the Authority shall be recorded in writing and be kept as a record.

14. Independence and Confidentiality.—(1) Members of the Authority shall make a commitment to attend and participate in its meetings.

(2) Every Member shall submit at each meeting of the Authority a Specific Declaration of Interest in Schedule I, which might be considered prejudicial to their independence in relation to any of the items on the agenda.

(3) Any Member or any other participant in a meeting, who believes that his interests may undermine his independence, shall inform the Chairperson in writing who thereon shall take a decision on his participation in the discussions at the meetings or the work of the Authority.

(4) Members of the Authority and invitees shall sign an initial Declaration at the first meeting of the Authority for maintaining the confidentiality of the business transacted at meetings of the Authority in Schedule II.

15. Secretariat.—Chief Executive Officer shall ensure appropriate administrative support to enable the Authority to carry out its work.

16. Reimbursement of expenses.—Special invitees to any meeting of the Authority shall be entitled to a payment of two thousand rupees for attending each meeting and the reimbursement of actual travel and subsistence expenses.

17. Removal of difficulty.—In the matter of implementation of these regulations or matters relating to interpretation thereof, if any doubt or difficulty arises, the same shall be placed before the Authority and the decision of the Authority thereon shall be final.
SCHEDULE I
[See regulation 14(2)]
SPECIFIC DECLARATION OF INTERESTS

Name: ........................................
Profession: ...................................

Meeting of the Unique Identification Authority of India

<table>
<thead>
<tr>
<th>Meeting dates</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Venue</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Agenda Items</th>
<th>Whether the member has a conflict of interest. (YES/NO) If yes, please provide details to enable the chair to take a decision.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Declaration: I declare that the information provided above is true and complete.
Done at .................................................. on this ........................................ day of ........................................

Signature........................................

SCHEDULE II
[See regulation 14(4)]
DECLARATION CONCERNING CONFIDENTIALITY

Name: ........................................
Position:
[ ] Member of the Unique Identification Authority of India
[ ] Other expert (external)
on ........................................

I hereby declare that I am aware of my obligation to respect confidentiality. I know that I am obliged not to divulge information acquired as a result of my activities in Unique Identification Authority of India, if the information is subject to a request for confidentiality and I hereby undertake not to divulge any such confidential information. I shall also respect the confidential nature of the opinions expressed by other Members or other experts during discussions in meetings or provided in written form.

Done at .................................................. on this ........................................ day of ........................................

Signature........................................
THE AADHAAR (ENROLMENT AND UPDATE) REGULATIONS, 2016

In exercise of the powers conferred by sub-section (1), and sub-clauses (a), (b), (d), (e), (j), (k), (l), (m), (r), (s) and (v) 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 (Enrolment and Update) Regulations, 2016 (1 of 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 Letter” means a document for conveying the Aadhaar number to a resident;

(c) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;

(d) “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;

(e) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;

(f) “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;

(g) “enrolling agency” means an agency appointed by the Authority or a Registrar, as the case may be, for collecting demographic and biometric information of individuals under the Act;

(h) “enrolment” means the process, as specified in these regulations, to collect demographic and biometric information from individuals by


2. Came into force on 14-9-2016.
the enrolling agencies for the purpose of issuing Aadhaar numbers
to such individuals under the Act;
(i) “enrolment centre” means a permanent or temporary centre set up
by an enrolling agency for carrying out enrolment of residents and
updating their information;
(j) “Enrolment ID” or “EID” means a 28 digit Enrolment Identification
Number allocated to residents at the time of enrolment;
(k) “Head of Family” means any member of a family of a resident in
respect of whom a document evidencing proof of relationship with
the resident can be furnished, and could include father, mother or
spouse of the resident;
(l) “identity information” in respect of an individual, includes his
Aadhaar number, his biometric information and his demographic
information;

1[(la) “Incapacitated Person” for the purpose of this Regulation, means a
person who is unable by reason of any physical or mental condition
to receive and evaluate information or to communicate decisions;]

(m) “introducer” means persons authorised by Registrars to introduce
residents who do not possess any of the prescribed supporting
documents;

(n) “operator” means the certified personnel employed by enrolling
agencies to execute the process of enrolment at the enrolment
centers;

(o) “Registrar” means any entity authorised or recognised by the
Authority for the purpose of enrolling individuals under this Act;

(p) “regulations” means the Aadhaar (Enrolment and Update)
Regulations, 2016;

(q) “resident” means 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;

(r) “service provider” includes all entities engaged for discharging any
function related to the enrolment or update process;

(s) “supervisor” means the certified personnel employed by enrolling
agencies to operate and manage the enrolment centres;

(t) “verifier” means the personnel appointed by Registrars for verification
of documents at enrolment centres;

(2) All other words and expressions used in these regulations but not defined,
and defined in the Act and the rules and other regulations made there under,
shall have the meanings respectively assigned to them in the Act or the rules
or other regulations, as the case may be.

CHAPTER II
RESIDENT ENROLMENT PROCESS

3. Biometric information required for enrolment.—(1) The following
biometric information shall be collected from all individuals undergoing
enrolment (other than children below five years of age):

1. Ins. by Notification No. 13012/79/2017/Legal-UlDAI (13) (No. 2 of 2018), dated 31st July,
2018 (w.e.f. 31-7-2018).
(i) Facial image;
(ii) All ten fingerprints; and
(iii) Scans of both irises.
(2) The standards for collecting the biometric information shall be as specified by the Authority for this purpose.

4. Demographic information required for enrolment.—(1) The following demographic information shall be collected from all individuals undergoing enrolment (other than children below five years of age):
   (i) Name;
   (ii) Date of Birth;
   (iii) Gender;
   (iv) Residential Address.
(2) The following demographic information may also additionally be collected during enrolment, at the option of the individual undergoing enrolment:
   (i) Mobile number;
   (ii) Email address.
(3) In case of Introducer-based enrolment, the following additional information shall be collected:
   (i) Introducer name;
   (ii) Introducer’s Aadhaar number.
(4) In case of Head of Family based enrolment, the following additional information shall be collected:
   (i) Name of Head of Family;
   (ii) Relationship;
   (iii) Head of Family’s Aadhaar number;
   (iv) One modality of biometric information of the Head of Family.
(5) The standards of the above demographic information shall be as may be specified by the Authority for this purpose.
(6) The demographic information shall not include race, religion, caste, tribe, ethnicity, language, record of entitlement, income or medical history of the resident.

5. Information required for enrolment of children below five years of age.—(1) For children below the five years of age, the following demographic and biometric information shall be collected:
   (a) Name;
   (b) Date of Birth;
   (c) Gender;
   (d) Enrolment ID or Aadhaar number of any one parent, preferably that of the mother in the event both parents are alive, or guardian. The Aadhaar number or EID of such parent or guardian is mandatory, and a field for relationship will also be recorded.
   (e) The address of such child which is the same as that of the linked parent/guardian.
   (f) Facial image of the child shall be captured. The biometric information of any one parent/guardian shall be captured or authenticated during the enrolment.
(2) The Proof of Relationship (PoR) document as listed in schedule II for establishing the relationship between the linked parent/guardian and the child.
shall be collected at the time of enrolment. Only those children can be enrolled based on the relationship document (PoR), whose names are recorded in the relationship document.

6. Enrolment of residents with biometric exceptions.—(1) For residents who are unable to provide fingerprints, owing to reasons such as injury, deformities, amputation of the fingers/hands or any other relevant reason, only iris scans of such residents will be collected.

(2) For residents who are unable to provide any biometric information contemplated by these regulations, the Authority shall provide for handling of such exceptions in the enrolment and update software, and such enrolment shall be carried out as per the procedure as may be specified by the Authority for this purpose.

7. Role of Registrars, enrolling agencies, etc., in enrolment.—(1) The Registrars appointed by the Authority shall carry out the enrolment of residents by themselves or through enrolling agencies contracted/appointed by them.

(2) The enrolling agencies shall set up enrolment centres for enrolment of residents as well as for correction or update of residents’ information. The opening of enrolment centres, the services offered and other guidelines for their operations shall be in accordance with the procedure as may be specified by the Authority for this purpose.

(3) Enrolment shall be carried out at permanent enrolment centres and through temporary centres set up for this purpose.

(4) Enrolment shall be carried out by the operators, verifiers, supervisors and other authorized personnel at the enrolment centres.

(5) Registrars shall make reasonable efforts to enrol residents who do not possess any of the prescribed supporting documents, through alternate modes of enrolment specified in regulation 10.

8. Equipment, software, etc., used in enrolment.—(1) The Registrars and enrolling agencies shall use only the software provided or authorised by the Authority for enrolment purposes.

(2) The standard enrolment/update software shall have the security features as may be specified by the Authority for this purpose.

(3) All equipment used in enrolment, such as computers, printers, biometric devices and other accessories shall be as per the specifications issued by the Authority for this purpose.

(4) The biometric devices used for enrolment shall meet the specifications, and shall be certified as per the procedure, as may be specified by the Authority for this purpose.

9. Disclosure of information to residents at the time of enrolment.—At the time of enrolment, the enrolling agency shall inform the individual undergoing enrolment of the following details:

(a) the manner in which the information shall be used;

(b) the nature of recipients with whom the information is intended to be shared during authentication; [*][**]

(c) the existence of a right to access information, the procedure for making requests for such access, and details of the person or department in-charge to whom such requests can be made. The above details shall be communicated to residents through the enrolment form, in a format provided in Schedule I [*][**]

1. The word "and" omitted by Notification No. 13012/79/2017/Legal-UIDAI (13) (No. 2 of 2018), dated 31st July, 2018 (w.e.f. 31-7-2018).

[(d) in case of an individual who has not attained the age of majority that is eighteen years, enrolling agency shall make disclosure of information in accordance with Regulation 9(a), (b) and (c) to parent/guardian of such minor; and]

[(e) in case a person is incapacitated, enrolling agency shall make disclosure of information in accordance with Regulation 9(a), (b) and (c) to the Legal Guardian appointed by Court or under any other law for the incapacitated person.]

10. Submission and verification of information.—(1) Residents seeking enrolment shall be required to submit an application for enrolment along with copies of supporting documents for proof of identity, address and date of birth, at an enrolment centre.

(2) An indicative list of supporting documents accepted for verification of identity, address and date of birth is prescribed in Schedule II. The Authority may expand or modify the list of acceptable supporting documents through circulars or notifications from time to time.

(3) The Authority may dispense with requirement of collecting proof of address and proof of identity of the residents in case of enrolment/update by Registrar General of India.

(4) In the event a resident does not possess any of the required supporting documents, enrolment may be carried out through the following modes:

(a) Introducer-based enrolment: If a resident is unable to provide documentary proof of identity or proof of address, he can be enrolled through a pre-designated introducer identified and notified by the Registrar or the regional offices of the Authority. Persons registered with the Authority as introducers could include the Registrars own employees, elected local body members, members of local administrative bodies, postman, influencers such as teachers, health workers, doctors, aanganwadis/asha workers, representatives of local NGOs. Such approved introducers shall introduce a resident and vouch for the validity of resident's information. An introducer shall verify the information filled, fill up his name and Aadhaar number, and affix his signature or thumb impression on the resident's enrolment form.

(b) Head of Family (HoF) based enrolment: In the event the head of family of a resident possesses the required supporting documents and has been enrolled through such supporting documents, the resident may be enrolled through such documents provided that (i) the resident can furnish proof of relationship, and (ii) the proof of relationship and the supporting documents record the same address for the family member and the head of family.

(5) The verification of the enrolment data in the above three methods shall be as provided in Schedule III.

11. Collection of information at enrolment centres.—(1) The enrolment operator shall capture (i) the demographic information as submitted by the resident in the application form; and (ii) the biometric information using the enrolment software provided or approved by the Authority.

(2) The enrolment operator shall collect and record the physical copies of the requisite supporting documents, or, if facility exists at the enrolment centre,
convert the physical copies into electronic format, as per the process as may be specified by the Authority.

(3) After capturing the information, a resident shall be given the opportunity of verifying his information for accuracy.

(4) On completion of enrolment, an acknowledgement slip containing the EID and other enrolment details signed by the enrolment operator shall be provided to the resident.

(5) The procedures, standards and guidelines to be followed during enrolment (including for enrolment of children below five years of age and for exception handling) and formats, templates, checklists to be used for carrying out enrolment shall be as per procedures as may be specified by the Authority for this purpose.

12. Agencies requiring Aadhaar as condition for receipt of service, etc.—Any Central or State department or agency which requires an individual to undergo authentication or furnish proof of possession of Aadhaar number as a condition for receipt of any subsidy, benefit or service pursuant to section 7 of the Act, shall ensure enrolment of its beneficiaries who are yet to be enrolled for update their Aadhaar details, through appropriate measures, including co-ordination with Registrars and setting up enrolment centres at convenient locations or providing enrolment facilities by becoming a Registrar itself.

12A. [Entitles requiring Aadhaar as condition for fulfilment 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 fulfilment 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.]

CHAPTER III
GENERATION OF AADHAAR NUMBERS AND DELIVERY TO RESIDENTS

13. Generation of Aadhaar numbers.—(1) The registrars and enrolling agencies shall upload the enrolment packet to the CIDR using the software provided by the Authority.

(2) The Authority shall process the enrolment data received from the Registrar and after the duplication and other checks as specified by the Authority, generate the Aadhaar number.

14. Rejection of enrolment.—(1) The Authority may reject an enrolment due to there being duplicate enrolments by the resident, quality or any other technical reason.

(2) In case of rejection due to duplicate enrolment, resident may be informed about the enrolment against which his Aadhaar number has been generated in the manner as may be specified by the Authority.

1. Ins. by Notification No. 13012/79/2017/Legal-UIDAI (No. 2 of 2017), dated 7th July, 2017 (w.e.f. 7-7-2017).
3. Subs. by Notification No. 13012/79/2017/Legal-UIDAI (No. 3 of 2017), dated 11th July, 2017, for "or agency" (w.e.f. 11-7-2017).
15. Delivery of Aadhaar number.—(1) The Aadhaar number may be communicated to residents in physical form (including letters or cards) and/or electronic form (available for download through the Authority’s website or through SMS).

(2) All agencies engaged by the Authority for printing, dispatch, and other functions related to delivery shall comply with the applicable processes.

CHAPTER IV

UPDATE OF RESIDENT INFORMATION

16. Request for update of identity information.—An Aadhaar number holder may seek alteration of his demographic information or biometric information in cases specified under section 31 of the Act in accordance with update procedure specified in this Chapter.

17. Mandatory update for children.—The Authority shall require the biometric information of children to be updated upon attaining five years of age and fifteen years of age in accordance with the procedure specified by the Authority.

18. Equipment, software, etc. used for update.—(1) The Registrars, enrolling agencies or other service providers involved in the update process shall use only the software provided or approved by the Authority for updating purposes.

(2) The standard update software shall have the security features as laid down by the Authority for this purpose.

(3) All equipment used for updating purposes, such as computers, printers, biometric devices and other accessories shall be as per specifications laid down by the Authority from time to time.

19. Mode of updating residents' information.—The process of updating residents' information in the CIDR may be carried out through the following modes:

(a) At any enrolment centre with the assistance of the operator and/or supervisor. The resident will be biometrically authenticated and shall be required to provide his Aadhaar number along with the identity information sought to be updated.[1]

[Provided that the date of birth of resident can be updated only once. In case the date of birth is to be updated more than once, it can only be done through an exception handling process which may require the resident to visit the Regional Office (RO) of the UIDAI.]

(b) Online mode: [Address] information may be updated online through designated portals upon submission of Aadhaar number and the registered mobile number. Authentication will be carried out through a One-Time Password (OTP) sent to the registered mobile number.

(c) Address Update using Aadhaar Address Update PIN service: Residents who are not having acceptable proof of Address may submit their request for address verification through Aadhaar letter.

---

4. Subs. by Notification No. 13012/79/2017/Legal-UIDAI (13) (No. 2 of 2018), dated 31st July, 2018, for regulation 19(c) (w.e.f. 31-7-2018). Regulation 19(c), before substitution, stood as under:

“(c) Postal mode: An update request for demographic information may also be sent in the format specified in Schedule IV through post along with the requisite supporting documents for verification.”.
having secret PIN. Once the letter is received by the resident, he/she can use the secret PIN to update his/her address in Aadhaar on the SSUP online portal.

The resident shall be assigned an update ID for tracking the status update, and the revised Aadhaar letter may be made available to the resident in physical or electronic form in accordance with the procedure as may be specified by the Authority for this purpose. The procedures for update, standards and guidelines to be followed along with the formats, templates, checklist to be used for carrying the update shall be as may be specified by the Authority for this purpose.

19A. Verification of update data.—Verification of the update data through the modes of updating residents’ information prescribed at Regulation 19 shall be as provided in the Schedule III.

20. Levy and collecting Fees.—The Authority may authorise Registrars, Enrolling Agencies and other Service Providers to collect a fee from the residents, not exceeding an amount specified by the Authority, for the services provided by them under the Act.

CHAPTER V

APPOINTMENT OF REGISTRARS, ENROLLING AGENCIES AND OTHER SERVICE PROVIDERS

21. Appointment of Registrars.—(1) Registrars shall be appointed by the Authority, through MOUs or agreements [or terms of appointment/engagement], for enrolment and update of residents across the country, and could include entities which interact with residents in the usual course of implementation of their programmes. The eligible entities for appointment as registrars are State/UT Governments, Central ministries and departments/agencies under them, Public Sector companies of Central/State Governments, [Scheduled banks] and regulated entities including National Securities Depository Limited, UTI Infrastructure Technology and Services Ltd., Special Purpose Vehicles (SPV) created by Central or State Government including CSC e-Governance services India Ltd. Upon appointment, a Registrar code shall be assigned to each Registrar.

(2) Registrars shall be responsible for field level execution, monitoring and audit.

(3) Registrars shall allow the Authority reasonable access to the premises occupied by it or by any other person on its behalf and also extend reasonable facility for examining any books, records, documents and computer data in the possession of the Registrar or any other person on their behalf and also provide copies of the document or other materials which, in the opinion of the Authority are relevant for the purpose of audit.

(4) Registrars shall not use the information collected during enrolment for any purpose other than uploading information to the CIDR.

1. Ins. by Notification No. 13012/79/2017/Legal-UIDAI (13) (No. 2 of 2018), dated 31st July, 2018 (w.e.f. 31-7-2018).
   "20. Convenience fee.—The Authority may authorise Registrars to charge convenience fee from the residents, not exceeding an amount specified by the Authority, for update of demographic information and biometric information."
(5) Registrars shall display on their websites adequate and appropriate information about enrolment and update services, including contact details of persons and services available to residents.

(6) Registrars shall ensure that any agency and/or person employed or appointed by them to conduct the enrolment and update operations is fit and proper and otherwise qualified to act, in the capacity so employed or appointed including having relevant professional training or experience.

(7) Registrars shall not permit sub-contracting of enrolment functions by enrolling agencies to third parties. Registrars may permit field level manpower to be hired through third parties provided the enrolling agencies furnishes details of the entities from which such manpower is sought to be hired.

(8) Registrars shall at all times abide by the Code of Conduct as specified in Schedule V of these regulations.

(9) Registrars shall adhere to the processes, policies and guidelines, checklists, forms and templates issued by the Authority from time to time and shall also ensure compliance by the enrolling agencies of such procedures, etc.

22. Registrars engaged before commencement of these regulations.—(1) The Registrars engaged prior to commencement of these regulations shall be deemed to be appointed as Registrars by the Authority under the Act:

Provided that the agreements entered into with them 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 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) In the event any Registrar engaged prior to commencement of these regulations wishes to cease being a Registrar under the Act, it may apply to the Authority in a form as may be specified by the Authority for this purpose, and shall cease to be a Registrar and to have the power to conduct enrolment or engage enrolling agencies for enrolment.

23. Empanelment of Enrolling Agencies.—(1) The Authority shall empanel the enrolling agencies through an open Request for Empanelment (RFE) process and the eligibility, terms and conditions of the empanelment shall be notified by the Authority from time to time.

(2) The interested agencies may apply for empanelment by fulfilling the eligibility and other technical and financial criteria of the RFE.

(3) The Authority shall evaluate the applications of agencies and empanel the eligible agencies as enrolling agencies after completing the requirements of the RFE.

(4) The Authority shall provide an Enrolling Agency Code using which the Registrar can onboard an empaneled enrolling agency to the CIDR.

(5) The Authority may also permit Registrars to engage other agencies as enrolling agencies after following a suitable process for screening and engaging such agencies, as may be specified by the Authority for this purpose.

(6) The enrolling agency shall be responsible for field level execution and audit. The enrolling agency shall allow the Authority reasonable access to the premises occupied by it or by any other person on its behalf and also extend reasonable facility for examining any books, records, documents and computer data in the possession of enrolling agency or any other person on their behalf and also provide copies of the document or other materials which, in the opinion of the Authority are relevant for the purpose of audit.

(7) The enrolling agencies shall not use the information collected during enrolment for any purpose other than uploading information to the CIDR.
(8) Enrolling agencies shall ensure that any agency and/or person employed or appointed by them to conduct the enrolment and update operations is fit and proper and otherwise qualified to act, in the capacity so employed or appointed, including having relevant professional training or experience.

(9) The enrolling agencies shall at all times abide by the Code of Conduct for service providers as specified in Schedule V of these regulations.

(10) The enrolling agencies shall adhere to the various process, policies and guidelines, checklists, forms and templates issued by the Authority from time to time.

(11) The enrolling agencies empaneled by the Authority prior to establishment of the Authority under the Act shall be deemed to have been empaneled as enrolling agencies by the Authority under the Act.

24. Other service providers.—(1) Other service providers may be appointed or engaged by the Authority from time to time for discharging any function related to the resident enrolment process or updating of information.

(2) All such service providers shall adhere to the regulations, processes, standards, guidelines, and orders issued by the Authority from time to time, and the code of conduct provided in Schedule V of these regulations, as applicable.

25. Testing and certification of staff appointed for enrolment.—(1) An enrolling agency shall ensure that the operators, supervisors, and other enrolment staff employed or engaged by it are duly certified for carrying out enrolment through a certification process as may be specified by the Authority.

(2) The Authority may designate testing and certification agencies for this purpose.

(3) The Authority may specify the minimum qualifications required for being engaged for any of the roles in the enrolment process, the process of their appointment, and the detailed roles and responsibilities of such personnel.

26. Liability of Registrars, enrolling agencies and other service providers and action in case of default.—(1) The Registrars, enrolling agencies, and other service providers, and the supervisors, operators or any other persons or agencies employed by them shall adhere to all regulations, processes, standards, guidelines, and orders issued by the Authority from time to time, and the code of conduct provided in Schedule V.

(2) The Authority shall monitor the enrolment activities of the Registrars, enrolling agencies and the operators, supervisors and other personnel associated with enrolment.

1[(3) Without prejudice to any other action which may be taken under the Act, for violation of any regulation, process, standard, guideline or order, by a Registrar or Enrolment Agency or any service provider or any other person, the Authority may immediately suspend the activities of such a Registrar or

---

1. Subs. by Notification No. 1302/79/2017/Legal-UIDAI (No. 5 of 2017), dated 31st July, 2017, for regulation 26(3) (w.e.f. 31-7-2017). Regulation 26(3), before substitution stood, as under:

"(3) Without prejudice to action that may be taken under the Act, violation of any regulation, process, standard, guideline or order by any service provider or other person may result in immediate suspension of the activities of such service providers or the concerned persons, and after holding due inquiry as deemed fit by the Authority, cancellation of their credentials, codes and permissions issued to them pursuant to the Act or these regulations.".
Enrolment Agency or service provider or concerned person, and after holding due enquiry, it may take steps for imposition of financial disincentives on such a Registrar or Enrolment Agency or service provider or any other person and for cancellation of the credentials, codes and permissions issued to them pursuant to the Act or these regulations, or any other steps as may be specifically provided for in the terms of engagement with the Authority.

CHAPTER VI
OMISSION OR DEACTIVATION OF AADHAAR NUMBER AND IDENTITY INFORMATION

27. Cases requiring omission of Aadhaar Number.—(1) The Aadhaar number of an Aadhaar number holder shall be cancelled in the following circumstances:

(a) If it is established that more than one Aadhaar numbers have been issued to the same person, then the Aadhaar number assigned from the earlier enrolment shall be retained, and all subsequent Aadhaar numbers shall be cancelled.

(b) Where the Aadhaar number has been generated in violation of the prescribed guidelines:

(i) "Photo on Photo" case where core biometric information is not available: Where an existing photograph is used for enrolment instead of capturing a new photograph at the enrolment centre, and where core biometric information has not been captured during enrolment, the resident's Aadhaar number shall be cancelled.

(ii) "False Biometric Exception" cases: Where the enrolment has been wrongly carried out as a 'biometric exception' case, the Aadhaar number shall be cancelled.

(iii) Where an adult has been enrolled as a child below five years of age to avoid capturing of biometric information, Aadhaar number shall be cancelled.

(iv) Any other case requiring cancellation owing to the enrolment appearing fraudulent to the Authority.

(2) Upon cancellation, services that are provided by the Authority to the Aadhaar number holder shall be disabled permanently.

28. Cases requiring deactivation of Aadhaar Number.—(1) The Aadhaar number of an Aadhaar number holder shall be deactivated in the following circumstances:

(a) "Photo on Photo" and core biometric information is available: Where an existing photograph is used instead of capturing a fresh photograph at the enrolment centre, and where core biometric information of the resident has been captured, the Aadhaar number shall be de-activated, and the resident asked to update his photograph. Upon successful update of his photograph, the Aadhaar number may be re-activated.

(b) "False Partial Biometric Exception" cases: Where certain attributes constituting biometric information have not been captured despite the resident being in a position to provide them, the Aadhaar number shall be de-activated.
(c) Where it is found at a later stage that enrolment has been carried out without valid supporting documents, the Aadhaar number shall be deactivated till it is updated by the Aadhaar number holder after furnishing valid supporting documents.

(d) Where the information captured has been flagged as having bad data and requiring update (such as mixed/anomalous biometrics information, abusive/expletive words and unparliamentary language in resident demographics, multiple names in single name using ‘urf’ or ‘Alias’), the Aadhaar number shall be deactivated till it is updated by Aadhaar holder.

(e) Where a child having attained the age of five or fifteen years of age fails to update his biometric information within two years of attaining such age, his Aadhaar number shall be deactivated. In cases where such update has not been carried out at the expiry of one year after deactivation, the Aadhaar number shall be omitted.

(f) Any other case requiring deactivation as deemed appropriate by the Authority.

(2) Upon deactivation, services that are provided by the Authority to the Aadhaar number holder shall be discontinued temporarily till such time the Aadhaar number holder updates or rectifies the information, owing to which his Aadhaar number has been deactivated by the Authority.

29. Inquiry into cases requiring omission or deactivation.—(1) Any case reported or identified as a possible case requiring omission or deactivation may require field inquiry which may include hearing the persons whose Aadhaar number is sought to be omitted or deactivated.

(2) An agency nominated by the Authority shall examine/inquire and submit a report to the Authority as per the procedures as may be specified by the Authority for this purpose.

(3) The Authority may initiate necessary action upon receiving the report and the decision to omit or deactivate an Aadhaar number shall lie with the Authority.

30. Communication to the Aadhaar number holder.—(1) An Aadhaar number holder shall be informed of the omission or deactivation of their Aadhaar number along with reasons through SMS, registered e-mail ID, tele-calling, letter or through such means as deemed fit by the Authority.

(2) Any complaint of an Aadhaar number holder in respect of such omission or deactivation may be addressed through the grievance redressal mechanism set up by the Authority.

31. Rectification action.—(1) In case of omission of Aadhaar number for reasons other than multiple Aadhaar numbers having been issued, residents shall be required to re-enrol.

(2) In case of deactivation, a resident shall be required to update his identity information partly or fully as required, as per the guidelines or policies as may be specified by the Authority.
CHAPTER VII
GRIEVANCE REDRESSAL MECHANISM

32. Setting up of a contact centre for grievance redressal.—(1) The Authority shall set up a contact centre to act as a central point of contact for resolution of queries and grievances of residents, accessible to residents through toll free number(s) and/or e-mail, as may be specified by the Authority for this purpose.

(2) The contact centre shall:
(a) Provide a mechanism to log queries or grievances and provide residents with a unique reference number for further tracking till closure of the matter;
(b) Provide regional language support to the extent possible;
(c) Ensure safety of any information received from residents in relation to their identity information;
(d) Comply with the procedures and processes as may be specified by the Authority for this purpose.

(3) Residents may also raise grievances by visiting the regional offices of the Authority or through any other officers or channels as may be specified by the Authority.

CHAPTER VIII
MISCELLANEOUS

33. 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.

34. Power to issue policies, process documents, etc.—The Authority may issue policies, orders, processes, standards, specifications and other documents, not inconsistent with these regulations, which are required to be specified under these regulations or for which provision is necessary for the purpose of giving effect to these regulations.

35. 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 I

### FORMAT FOR ENROLMENT FORM

(See regulation 9 of these Regulations)

**AADHAAR ENROLMENT/CORRECTION FORM**

AADhaar Enrolment is free and voluntary. Correction within 96 hours of enrolment is also free. No charges are applicable for Form and Aadhaar Enrolment. In case of Correction provide your EID, Name and only that field which needs Correction.

In case of Correction provide your:

<table>
<thead>
<tr>
<th>EID No. here</th>
<th>dd/mm/yyyy</th>
<th>hh:mm:ss</th>
</tr>
</thead>
</table>

Please follow the instructions overleaf while filling up the form.

Use capital letters only.

<table>
<thead>
<tr>
<th>1</th>
<th>Pre-Enrolment ID :</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>NPR Receipt/TIN Number:</td>
</tr>
<tr>
<td>3</td>
<td>Full Name:</td>
</tr>
<tr>
<td>4</td>
<td>Gender: Male ( ) Female ( ) Transgender ( )</td>
</tr>
<tr>
<td>5</td>
<td>Age: Yrs or Date of Birth: DD/MM/YYYY Declared ☐ Verified ☐</td>
</tr>
<tr>
<td>6</td>
<td>Address: C/o ( ) D/o ( ) S/o ( ) W/o ( ) H/o ( ) NAME</td>
</tr>
<tr>
<td></td>
<td>House No./ Bldg./ Apt.</td>
</tr>
<tr>
<td></td>
<td>Street/Road/Lane</td>
</tr>
<tr>
<td></td>
<td>Landmark</td>
</tr>
<tr>
<td></td>
<td>Area/locality/sector</td>
</tr>
<tr>
<td></td>
<td>Village/Town/City</td>
</tr>
<tr>
<td></td>
<td>Post Office</td>
</tr>
<tr>
<td></td>
<td>District</td>
</tr>
<tr>
<td></td>
<td>Sub-District</td>
</tr>
<tr>
<td></td>
<td>State</td>
</tr>
<tr>
<td></td>
<td>E-Mail</td>
</tr>
<tr>
<td></td>
<td>Mobile No.</td>
</tr>
<tr>
<td></td>
<td>PIN CODE</td>
</tr>
</tbody>
</table>

7. Details of: Father ( ) Mother ( ) Guardian ( ) Husband ( ) Wife ( ) For children below 5 years Father/Mother/Guardian’s details are mandatory. Adults can opt to not specify this information, if they cannot/do not want to disclose.

Name

<table>
<thead>
<tr>
<th>EID/Aadhaar No.:</th>
<th>dd/mm/yyyy</th>
<th>hh:mm:ss</th>
</tr>
</thead>
</table>

Verification Type: Document Based ( ) Introducer Based ( ) Head of Family ( )

Select only one of the above. Select Introducer or Head of Family only if you do not possess any documentary proof of identity and/or address. Introducer and Head of Family details are not required in case of Document based Verification.

8. For Document Based (Write Names of the documents produced. Refer overleaf of this form for list of valid documents)

   a. POI
   b. POA
   c. DOB
   d. POR

(Mandatory in case of Verified Date of Birth)
For Introducer Based -
Introducer’s Aadhaar No.:

For HoF Based - Details of:
Mother’s Name:
Guardian’s Name:
Husband’s Name:
Wife’s Name:
HoF’s EID/Aadhaar No.:

I hereby confirm the identity and address of………………………as being true, correct and accurate.

Introducer/HoF’s Name:________________________ Signature of Introducer/HoF:

Disclosure under section 3(2) of THE AADHAAR (TARGETED DELIVERY OF FINANCIAL AND OTHER SUBSIDIES, BENEFITS AND SERVICES) ACT, 2016

I confirm that I have been residing in India for at least 182 days in the preceding 12 months & information (including biometrics) provided by me to the UIDAI is my own and is true, correct and accurate. I am aware that my information including biometrics will be used for generation of Aadhaar and authentication. I understand that my Identity information (except core biometric) may be provided to an agency only with my consent during authentication or as per the provisions of the Aadhaar Act. I have a right to access my Identity information (except core biometrics) following the procedure laid down by UIDAI.

Verifier’s Stamp and Signature:
(Verifier must put his/her Name, if stamp is not available)

Applicant’s signature/Thumbprint

To be filled by the Enrolment Agency only:

Field 2 NPR NUMBER Resident may bring his/her National Population Register Survey slip (if available) and fill up the column.

Field 3 NAME Write full name without salutations/titles. Please bring the original Proof of Identity (POI) document. (See list A below).

Field 5 DOB/AGE Fill in Date of Birth in DD/MM/YYYY format if exact Date of Birth is not known, approximate age in Years may be filled in the space provided. Please bring the original Proof of Date of Birth (DoB), if available (See list D below). Declared checkbox may be selected if Resident does not have a valid proof of Date of Birth document. Verified checkbox is selected where Resident has provided documents as proof of Date of Birth.

Field 6 ADDRESS Write complete address. Please bring the original Proof of Address (POA) document. (See list B below). Please note that the Aadhaar letter will be delivered at the given address only.

- To include Parent/Guardian/Spouse name as part of the address, select the appropriate box and enter the name of the person.

- Minor Corrections/Enhancements are permissible to make the address complete without altering the base address as mentioned in the POA document.
Field 7: RELATIONSHIP
- In case of children below 5 years, it is mandatory to provide father/mother guardian details with their Aadhaar or EID number.
- If the resident is not holding a Proof of Identity & using the Head of the Family identity for enrolment, it is mandatory to provide Head of the family’s details with his/her Aadhaar or EID number. Please refer Illustration below for filling EID. Please bring the original Proof of Relationship (POR) document. (See list C below).
- For other cases, it is optional for the resident to fill up the relationship details.

Field 8: DOCUMENTS
Write the name of Documents for PoI and PoA. In case proof of Date of Birth is available, then write the name of Date of Birth document. If the resident is not holding a Proof of Identity & using the Head of Family based enrolment, then write the name of Proof of Relationship document. For valid list of documents, please refer list of Documents below.

Field 9: INTRODUCER/ HoF
Resident who does not have PoI and PoA may get enrolled through an Introductor/Head of Family. Pl contact nearest enrolment centre or your Registrar, for further details.

List A. POI documents
1. Passport
2. PAN Card
3. Ration/PDS Photo Card
4. Voter ID
5. Driving License
6. Government Photo ID Cards/service photo identity card issued by PSU.
7. NREGS Job Card
8. Photo ID issued by Recognized Educational Institution.
9. Arms License
10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kissan Photo Passbook
15. CGHS/ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identity having photo issued by Gazetted Officer or Tehsildar on letterhead

List B. POA documents
1. Passport
2. Bank Statement/Passbook
3. Post Office Account Statement/Passbook
4. Ration Card
5. Voter ID
6. Driving License
7. Government Photo ID cards/service photo identity card issued by PSU
8. Electricity Bill (not older than 3 months)
9. Water bill (not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property Tax Receipt (not older than 3 months)
12. Credit Card Statement (not older than 3 months)
13. Insurance Policy
14. Signed Letter having Photo from Bank on letterhead
15. Signed Letter having Photo issued by registered Company on letterhead
### List A. POI documents
1. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations

### List B. POA documents
1. Signed Letter having Photo issued by Recognized Educational Instruction on letterhead
2. NREGS Job Card
3. Arms License
4. Pensioner Card
5. Freedom Fighter Card
6. Kissan Passbook
7. CGHS/ECHS Card
8. Certificate of Address having photo issued by MP or MLA or Gazetted Officer or Tehsildar on letterhead
9. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
10. Income Tax Assessment Order
11. Vehicle Registration Certificate
12. Registered Sale/Lease/Rent Agreement
13. Address Card having Photo issued by Department of Posts
14. Caste and Domicile Certificate having Photo issued by State Govt.
15. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
16. Gas Connection Bill (not older than 3 months)
17. Passport of Spouse
18. Passport of Parents (in case of Minor)

### List C. POR documents
1. PDS Card
2. MNREGA Job Card
3. CGHS/State Government/ECHS/BIS/Government card
4. Pension Card
5. Army Canteen Card
6. Passport

### List D. DOR documents
1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on letterhead
7. Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local government bodies like Taluk, Tehsil etc. (This is not Aadhaar number)

8. Any other Central/ State government issued family entitlement document

9. Marriage Certificate
   - Issued by the Government

*In instances where original documents are not available, copies, attested/certified by a public notary/gazetted officer will be accepted.

[Note.—In case of minor, the signature will be done by parent/guardian. In case of incapacitated person, the signature will be done by Legal Guardian of Incapacitated Person.]

[SCHEDULE II

LIST OF ACCEPTABLE SUPPORTING DOCUMENTS FOR VERIFICATION
(See regulation 10(2) of these Regulations)

1. Passport
2. PAN Card
3. Ration/ PDS Photo Card
4. Voter ID
5. Driving License
6. Government Photo ID Cards/ service photo identity card issued by PSU
7. NRC/ES/ ECHS Photo Card
8. Photo ID issued by Recognized Educational Institution
9. Arms License
10. Photo Bank ATM Card
11. Photo Credit Card
12. Pensioner Photo Card
13. Freedom Fighter Photo Card
14. Kisan Photo Passbook
15. CGHS / ECHS Photo Card
16. Address Card having Name and Photo issued by Department of Posts
17. Certificate of Identity having photo issued by Gazetted Officer or Tehsildar on letterhead
18. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
20. Certificate from Superintendent/ Warden/ Matron/ Head of Institution of recognized shelter homes for orphans, homes etc on their official letterhead
21. Certificate of Identity having photo issued by MP or MLA or MLC or Municipal Councillor on letterhead
22. Certificate of Identity having photo issued by village panchayat head or mukhiya (for rural areas)
23. Gazette notification for name change
24. Marriage certificate with photograph
25. RSBY Card
26. SSLC book having candidates photograph
27. ST/ SC/ OBC certificate with photograph
28. School Leaving Certificate (SLC) / School Transfer Certificate (TC), containing name and photograph

1. Ins. by Notification No. 13012/79/2017/Legal-UIDAI (13) (No. 2 of 2018), dated 31st July, 2018 (w.e.f. 31-7-2018).
29. Extract of School Records issued by Head of School containing name and photograph
30. Bank Pass Book having name and photograph
31. Certificate of Identity containing name and photograph issued by Recognized Educational Institution signed by Head of Institute

List B. POA (Proof of Address) documents containing Name and Address
1. Passport
2. Bank Statement/Passbook
3. Post Office Account Statement/Passbook
4. Ration Card
5. Voter ID
6. Driving License
7. Government Photo ID cards/service photo identity card issued by PSU
8. Electricity Bill (not older than 3 months)
9. Water Bill (not older than 3 months)
10. Telephone Landline Bill (not older than 3 months)
11. Property Tax Receipt (not older than 1 year)
12. Credit Card Statement (not older than 3 months)
13. Insurance Policy
14. Signed Letter having Photo from Bank on letterhead
15. Signed Letter having Photo issued by registered Company on letterhead
16. Signed Letter having Photo issued by Recognized Educational Institution on letterhead or Photo ID having address issued by Recognized Educational Institution
17. NREGS Job Card
18. Arms License
19. Pensioner Card
20. Freedom Fighter Card
21. Kissan Passbook
22. OGHIS / ECHS Card
23. Certificate of Address having photo issued by MP or MLA or MLC or Gazetted Officer or Tehsildar on letterhead
24. Certificate of Address issued by Village Panchayat head or its equivalent authority (for rural areas)
25. Income Tax Assessment Order
26. Vehicle Registration Certificate
27. Registered Sale / Lease / Rent Agreement
28. Address Card having Photo issued by Department of Posts
29. Caste and Domicile Certificate having Photo issued by State Govt
30. Disability ID Card/handicapped medical certificate issued by the respective State/UT Governments/Administrations
31. Gas Connection Bill (not older than 3 months)
32. Passport of Spouse
33. Passport of Parents (in case of Minor)
34. Allotment letter of accommodation issued by Central/State Govt. of not more than 3 years old
35. Marriage Certificate issued by the Government, containing address
36. Bramashah card
37. Certificate from Superintendent/ Warden/ Matron/ Head of Institution of recognized shelter homes for orphans, homes etc. on letterhead
38. Certificate of address having photo issued by Municipal Councillor on letterhead
39. Identity Card issued by recognized educational institutions
40. SSLC book having photograph
41. School Identity card
42. School Leaving Certificate (SLC) / School Transfer Certificate (TC), containing Name and Address
43. Extract of School Records containing Name, Address and Photograph issued by Head of School
44. Certificate of Identity containing Name, Address and Photograph issued by Recognized Educational Institution signed by Head of Institute
List C. POR (Proof of Relationship) documents containing Name of applicant and Name of HoF (Head of Family)
1. PDS Card
2. MNREGA Job Card
3. CGHS/State Government/ECHS/ESIC Medical card
4. Pension Card
5. Army Canteen Card
6. Passport
7. Birth Certificate issued by Registrar of Birth, Municipal Corporation and other notified local government bodies like Taluk, Tehsil etc.
8. Any other Central/State government issued family entitlement document
9. Marriage Certificate issued by the government
10. Address card having name and photo issued by Department of Posts
11. Bhamaushah card
12. Discharge card/slip issued by Government hospitals for birth of a child
13. Certificate of Identity having photo issued by MP or MLA or MLC or Municipal Councillor or Gazetted Officer on letterhead
14. Certificate of Identity having photo and relationship with HoF issued by village panchayat head or mukhiya (for rural areas)

List D. DOB (Date of Birth) documents containing Name and DOB
1. Birth Certificate
2. SSLC Book/Certificate
3. Passport
4. Certificate of Date of Birth issued by Group A Gazetted Officer on Letterhead
5. A certificate or ID Card having photo and Date of Birth (DOB) duly signed and issued by a Government authority
6. Photo ID card having Date of Birth, issued by Recognized Educational Institution
7. PAN Card
8. Marks sheet issued by any Government Board or University
9. Government Photo ID Card/Photo Identity Card issued by PSU containing DOB
10. Central/State Pension Payment Order
11. Central Government Health Service Scheme Photo Card or Ex-Servicemen Contributory Health Scheme Photo card
12. School Leaving Certificate (SLC) / School Transfer Certificate (TC), containing Name and Date of Birth
13. Extract of School Records issued by Head of School containing Name, Date of Birth and Photograph
14. Certificate of Identity containing Name, DOB and Photograph issued by Recognized Educational Institution signed by Head of Institute

SCHEDULE III
VERIFICATION OF ENROLMENT [AND UPDATE] INFORMATION
(See regulation 10(5) [and regulation 19A] of these Regulations)

<table>
<thead>
<tr>
<th>Information</th>
<th>Fields</th>
<th>Verification Required?</th>
<th>Verification Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal Details</td>
<td>Name</td>
<td>Yes</td>
<td>Any of the Proof of Identity documents.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o Introducer/Head of Family for people who have no documents.</td>
</tr>
<tr>
<td></td>
<td>Date of Birth</td>
<td><img src="https://via.placeholder.com/15" alt="" /></td>
<td>A flag is maintained to indicate if Date of Birth (DOB) is verified, declared, or approximate. <img src="https://via.placeholder.com/15" alt="" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>![Yes]</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>![Update of DOB is only allowed as Verified]</td>
</tr>
</tbody>
</table>

1. Ins. by Notification No. 13012/79/2017/Legal-UIDAI (13) (No. 2 of 2018), dated 31st July, 2018 (w.e.f. 31-7-2018).
<table>
<thead>
<tr>
<th><strong>Gender</strong></th>
<th><strong>Residential Address</strong> (for Aadhaar letter delivery and other communications)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No</strong></td>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>o Any of the Proof of Address documents.</td>
</tr>
<tr>
<td></td>
<td>o Introducer/Head of Family for people who have no documents.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Parent/Guardian Details</strong></th>
<th><strong>Father's/Mother's/Guardian's/Husband's/Wife's Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details</strong></td>
<td><strong>Conditional</strong></td>
</tr>
<tr>
<td></td>
<td>o No verification of Father/Husband/Guardian in the case of adults.</td>
</tr>
<tr>
<td></td>
<td>o For children below five years of age, Father/Mother/Guardian's name, Aadhaar number and biometric information (any one modality) shall be captured for authentication.</td>
</tr>
<tr>
<td></td>
<td>o For adults, Name of either Father/Husband/Guardian or Mother/Wife/Guardian is optional.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Introducer/Hol' Details</strong></th>
<th><strong>Introducer/Hol's Name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Details</strong></td>
<td><strong>Yes</strong></td>
</tr>
<tr>
<td></td>
<td>o Introducer/Hol's Name, UID on the form.</td>
</tr>
<tr>
<td></td>
<td>o Introducer/Hol's biometrics (any one modality) captured for authentication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Contact Details</strong></th>
<th><strong>Mobile Number</strong></th>
<th><strong>No</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Email Address</strong></th>
<th><strong>No</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**SCHEDULE IV**

1

**SCHEDULE V**

**CODE OF CONDUCT FOR SERVICE PROVIDERS**

1. Service Providers shall make best efforts to protect the interests of residents.
2. Service Providers shall maintain high standards of ethics, integrity, dignity and fairness in the conduct of Aadhaar enrolment and update of residents.
3. Service Providers shall fulfill their obligations in a prompt, ethical and professional manner.
4. Service Providers shall at all times exercise due diligence, ensure proper care and exercise independent professional judgment.
5. Service Providers shall not divulge to anybody either orally or in writing, directly or indirectly, any confidential information about the residents which has come to their knowledge, except where such disclosures are required to be made in compliance with the Act or any other law for the time being in force.

---

6. Service Providers shall not indulge in any unfair practice.
7. Service Providers shall ensure that grievances of residents are redressed in a timely and appropriate manner.
8. Service Providers shall make reasonable efforts to avoid misrepresentation and ensure that the information provided to the residents is not misleading.
9. Service Providers shall abide by the provisions of the Act and the rules, regulations issued by the Government and the Authority, from time to time, as may be applicable.
10. Service Providers shall not make untrue statements or suppress any material fact in any documents, reports, papers or information furnished to the Authority.
11. Service Providers shall ensure that the Authority is promptly informed about any action, legal proceeding, etc., initiated against it in respect of any material breach or non-compliance by it, of any law, rules, regulations and directions of the Authority or of any other regulatory body.
12. Service Providers shall be responsible for the acts or omissions of their agencies and employees in respect of the conduct of their enrolment and update services.
13. Service Providers should have adequately trained staff and arrangements to render fair, prompt and competent services to residents.
14. Service Providers shall develop their own internal code of conduct for governing internal operations and laying down standards of appropriate conduct for their agencies, employees and officers in the carrying out of their duties. Such a code may extend to the maintenance of professional excellence and standards, integrity, confidentiality, objectivity, and avoidance of conflict of interests.
15. Service Providers shall follow maker-checker concept in their activities to ensure accuracy of enrolment and update data.
16. Service Providers shall not indulge in manipulative, fraudulent practices in the process of enrolment and updation.
17. Service Providers shall ensure security and protection of all data (demographic/biometric) collected from residents in accordance with policies and processes as may be specified by the Authority for this purpose.
18. Service Providers shall enforce the decision of Authority regarding suspension/debarment/disempowerment of enrolling agencies, operators, supervisors etc., as applicable.
19. Service Providers shall follow the standards for data fields, data verification and biometric fields specified by the Authority.
20. Where required, Service Providers shall use only those devices and IT systems whose specifications have been approved by the Authority.
21. Service Providers shall follow the protocols prescribed by the Authority for record keeping and maintenance.
22. Service Providers shall follow the process and systems specified by the Authority for transmission of the data collected.
23. Service Providers shall follow the confidentiality, privacy and security protocols as may be specified by the Authority.
24. Service Providers shall follow protocols as may be specified by the Authority for spreading and communicating the message, content and intent of the Aadhaar project. Since the Aadhaar logo and brand name are properties of the Authority,
the Authority will specify the manner and limits of the use of the Authority logo, brand name, brand design and other communication and awareness materials.

25. Service Providers shall follow protocols, processes and standards specified by the Authority for the implementation of the Aadhaar processes.

26. Service Providers shall submit periodic reports of enrolment to the Authority in the form and manner as may be specified by the Authority.

27. Service Providers shall provide information related to the Aadhaar processes from time to time as requested by the Authority.
THE AADHAAR (AUTHENTICATION) REGULATIONS, 2016

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 1
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;

(h) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11 of the Act;


2. Came into force on 14-9-2016.
(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 Act or 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 fulfill 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 fulfill 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 P1D block which can then be transmitted in accordance with specifications and processes laid down by the Authority;
(c) the encrypted P1D 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 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 there under, 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

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.

27. Duration of storage.—(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.

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:

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Organisation Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1</td>
<td>Government Organisation</td>
</tr>
<tr>
<td>1.1</td>
<td>A Central/State Government Ministry/Department and their attached or sub-ordinate offices.</td>
</tr>
<tr>
<td>1.2</td>
<td>An undertaking owned and managed by Central/State Government (PSU)</td>
</tr>
<tr>
<td>1.3</td>
<td>An Authority constituted under the Central/State Act/Special Purpose Organisation constituted by Central/State govt.</td>
</tr>
<tr>
<td>Category 2</td>
<td>Regulated Service Providers</td>
</tr>
<tr>
<td>2.1</td>
<td>Regulated/Licensed by RBI* - Banks and Payment &amp; Settlement System</td>
</tr>
<tr>
<td></td>
<td>2.1.1 Public Sector Banks (PSB)</td>
</tr>
<tr>
<td></td>
<td>2.1.2 Private Banks, Foreign Banks Licensed by RBI to operate in India, Payment Banks, Small Finance Banks</td>
</tr>
<tr>
<td></td>
<td>2.1.3 Regional Rural Banks</td>
</tr>
<tr>
<td></td>
<td>2.1.4 Co-operative Banks</td>
</tr>
<tr>
<td></td>
<td>5. State Co-operative Banks</td>
</tr>
<tr>
<td></td>
<td>6. District Co-operative Banks</td>
</tr>
<tr>
<td></td>
<td>7. Scheduled Urban Co-operatives Banks</td>
</tr>
<tr>
<td></td>
<td>8. Non Scheduled Urban Co-operative Banks</td>
</tr>
<tr>
<td></td>
<td>2.1.5 Payment &amp; Settlement System Network</td>
</tr>
<tr>
<td></td>
<td>1. Financial market infrastructure</td>
</tr>
<tr>
<td></td>
<td>2. Retail payments Organisation</td>
</tr>
<tr>
<td></td>
<td>3. Cards payment network</td>
</tr>
<tr>
<td></td>
<td>4. ATM networks</td>
</tr>
<tr>
<td></td>
<td>5. Pre-paid payment instruments</td>
</tr>
<tr>
<td></td>
<td>6. White label ATM operators</td>
</tr>
<tr>
<td></td>
<td>7. Instant Money Transfer</td>
</tr>
<tr>
<td></td>
<td>2.1.6 Non-Banking Financial Company</td>
</tr>
<tr>
<td>2.2</td>
<td>Regulated by IRDA/PFRDA - Financial Institutions</td>
</tr>
<tr>
<td>2.3</td>
<td>Regulated by TRAI - Telecom</td>
</tr>
</tbody>
</table>
## 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

### 3.1 Other Entities

#### 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 India 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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Authentication User Agency (AUA)</th>
<th>Additional requirements for eKYC User Agency (KUA)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category 1</strong></td>
<td>Technical Requirements</td>
<td>Financial Requirements</td>
</tr>
<tr>
<td>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.</td>
<td>No financial requirement</td>
<td>No additional requirement for KUA</td>
</tr>
<tr>
<td><strong>Category 2</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Entity should have IT Infrastructure owned or outsourced capable of carrying out minimum 1 Lakh Authentication transactions per month.</td>
<td>No financial requirement</td>
<td>No additional requirement for KUA</td>
</tr>
<tr>
<td>3. Organisation should have a prescribed Data Privacy policy to protect beneficiary privacy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Organisation should have adopted data security requirements as per the IT Act, 2000.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Schedule B

**Eligibility Criteria of Authentication Service Agencies**

[See regulation 10(2)]

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

<table>
<thead>
<tr>
<th>Sl. No.</th>
<th>Organisation Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category 1</strong></td>
<td>A Central/State Government Ministry/Department or an undertaking owned and managed by Central/State Government</td>
</tr>
<tr>
<td><strong>Category 2</strong></td>
<td>An Authority constituted under the Central/State Act</td>
</tr>
<tr>
<td><strong>Category 3</strong></td>
<td>Any other entity of national importance as determined by the Authority</td>
</tr>
<tr>
<td><strong>Category 4</strong></td>
<td>A company registered in India under the Indian Companies Act, 1956</td>
</tr>
<tr>
<td><strong>Category 5</strong></td>
<td>AUA/KUA</td>
</tr>
</tbody>
</table>
The Aadhaar (Authentication) Regulations, 2016

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Financial Requirement</th>
<th>Technical Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Category 1, 2 and 3</td>
<td>No financial requirements</td>
<td>No technical requirements</td>
</tr>
<tr>
<td>Category 4</td>
<td>An annual turnover of at least 100 crores in last three financial years</td>
<td>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 state, 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,</td>
</tr>
<tr>
<td>Category 5</td>
<td>No Financial requirements</td>
<td>Any AUA or KUA meeting authentication transaction criteria as laid down by the Authority from time to time</td>
</tr>
</tbody>
</table>
(3) The Authority shall monitor compliance with the information security policy and other security requirements through internal audits or through independent agencies.

(4) The Authority shall designate an officer as Chief Information Security Officer for disseminating and monitoring the information security policy and other security-related programmes and initiatives of the Authority.

4. Security obligations of the personnel.—(1) The personnel shall comply with the information security policy, and other policies, guidelines, procedures, etc., issued by the Authority from time to time.

(2) Without prejudice to any action that may be taken under the Act, personnel may be liable to action in accordance with procedures specified by the Authority for this purpose:

Provided that no such action shall be taken without giving the concerned personnel a reasonable opportunity of being heard.

5. Security obligations of service providers, etc.—The agencies, consultants, advisors and other service providers engaged by the Authority for discharging any function relating to its processes shall:

(a) ensure compliance with the information security policy specified by the Authority;

(b) periodically report compliance with the information security policy and contractual requirements, as required by the Authority;

(c) report promptly to the Authority any security incidents affecting the confidentiality, integrity and availability of information related to the Authority’s functions;

(d) ensure that records related to the Authority shall be protected from loss, destruction, falsification, unauthorised access and unauthorised release;

(e) ensure confidentiality obligations are maintained during the term and on termination of the agreement;

(f) ensure that appropriate security and confidentiality obligations are provided for in their agreements with their employees and staff members;

(g) ensure that the employees having physical access to CIDR data centers and logical access to CIDR data centers undergo necessary background checks;

(h) define the security perimeters holding sensitive information, and ensure only authorised individuals are allowed access to such areas to prevent any data leakage or misuse; and

(i) where they are involved in the handling of the biometric data, ensure that they use only those biometric devices which are certified by a certification body as identified by the Authority and ensure that appropriate systems are built to ensure security of the biometric data.
6. Audits and inspection of service providers, etc.—(1) All agencies, consultants, advisors and other service providers engaged by the Authority, and ecosystem partners such as registrars, requesting entities, Authentication User Agencies and Authentication Service Agencies shall get their operations audited by an information systems auditor certified by a recognised body under the Information Technology Act, 2000 and furnish certified audit reports to the Authority, upon request or at time periods specified by the Authority.

(2) In addition to the audits referred to in sub-regulation (1), the Authority may conduct audits of the operations and systems of such entities or persons, either by itself or through an auditor appointed by the Authority.

7. Confidentiality.—All procedures, orders, processes, standards and protocols related to security, which are designated as confidential by the Authority, shall be treated as confidential by all its personnel and shall be disclosed to the concerned parties only to the extent required for giving effect to the security measures. The nature of information that cannot be shared outside the Authority unless mandated under the Act includes, but not limited to, Information in CIDR, Technology details, Network Architecture, Information security policy and processes, software codes, internal reports, audit and assessment reports, applications details, asset details, contractual agreements, present and future planned infrastructure details, protection services, and capabilities of the system.

8. Savings.—All procedures, orders, processes, standards 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.

9. Power to issue policies, process documents, etc.—The Authority may issue policies, processes, standards and other documents, not inconsistent with these regulations, which are required to be specified under these regulations or for which provision is necessary for the purpose of giving effect to these regulations.

10. Power to issue clarifications, guidelines and removal of difficulties.—In order to clarify any matter pertaining to application or interpretation of these regulations, or to remove any difficulties in implementation of these regulations, the Authority shall have the power to issue clarifications and guidelines in the form of circulars which shall have effect of these regulations.
THE AADHAAR (SHARING OF INFORMATION) REGULATIONS, 2016

In exercise of the powers conferred by sub-section (1), and sub-clause (c) of sub-section (2) of section 54 read with sub-clause (k) of sub-section (2) of section 23, and sub-sections (2) and (4) of section 29 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 (Sharing of Information) 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 Letter” means a document for conveying the Aadhaar number to a resident;

(c) “Aadhaar number holder” means an individual who has been issued an Aadhaar number under the Act;

(d) “Authority” means the Unique Identification Authority of India established under sub-section (1) of section 11;

(e) “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.

(2) All other words and expressions used in these regulations but not defined, and defined in the Act and the rules and other regulations made thereunder, shall have the meanings respectively assigned to them in the Act or the rules or other regulations, as the case may be.

CHAPTER II
REstrictions on sharing of identity information

3. Sharing of information by the Authority.—(1) Core biometric information collected by the Authority under the Act shall not be shared with anyone for any reason whatsoever.


2. Came into force on 14-9-2016.
(2) The demographic information and photograph of an individual collected by the Authority under the Act may be shared by the Authority with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual, upon the requesting entity obtaining consent from the Aadhaar number holder for the authentication process, in accordance with the provisions of the Act and the Aadhaar (Authentication) Regulations, 2016.

(3) The Authority shall share authentication records of the Aadhaar number holder with him in accordance with regulation 28 of the Aadhaar (Authentication) Regulations, 2016.

(4) The Authority may share demographic information and photograph, and the authentication records of an Aadhaar number holder when required to do so in accordance with section 33 of the Act.

4. Sharing of information by a requesting entity.—(1) Core biometric information collected or captured by a requesting entity from the Aadhaar number holder at the time of authentication shall not be stored except for buffered authentication as specified in the Aadhaar (Authentication) Regulations, 2016, and shall not be shared with anyone for any reason whatsoever.

(2) The identity information available with a requesting entity:

(a) shall not be used by the requesting entity for any purpose other than that specified to the Aadhaar number holder at the time of submitting identity information for authentication; and

(b) shall not be disclosed further without the prior consent of the Aadhaar number holder.

(3) A requesting entity may share the authentication logs of an Aadhaar number holder with the concerned Aadhaar number holder upon his request or for grievance redressal and resolution of disputes or with the Authority for audit purposes, as specified in regulation 18 of the Aadhaar (Authentication) Regulations, 2016.

5. Responsibility of any agency or entity other than requesting entity with respect to Aadhaar number.—(1) Any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall:

(a) collect, store and use the Aadhaar number for a lawful purpose;

(b) inform the Aadhaar number holder the following details:
   (i) the purpose for which the information is collected;
   (ii) whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it;
   (iii) alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any;

(c) obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes.

(2) Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent.
(3) Such individual, agency or entity shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder.

6. Restrictions on sharing, circulating or publishing of Aadhaar number.—
(1) The Aadhaar number of an individual shall not be published, displayed or posted publicly by any person or entity or agency.

(2) Any individual, entity or agency, which is in possession of Aadhaar number(s) of Aadhaar number holders, shall ensure security and confidentiality of the Aadhaar numbers and of any record or database containing the Aadhaar numbers.

(3) Without prejudice to sub-regulations (1) and (2), no entity, including a requesting entity, which is in possession of the Aadhaar number of an Aadhaar number holder, shall make public any database or record containing the Aadhaar numbers of individuals, unless the Aadhaar numbers have been redacted or blacked out through appropriate means, both in print and electronic form:

(4) No entity, including a requesting entity, shall require an individual to transmit his Aadhaar number over the Internet unless such transmission is secure and the Aadhaar number is transmitted in encrypted form except where transmission is required for correction of errors or redressal of grievances.

(5) No entity, including a requesting entity, shall retain Aadhaar numbers or any document or database containing Aadhaar numbers for longer than is necessary for the purpose specified to the Aadhaar number holder at the time of obtaining consent.

7. Liability for contravention of the regulations.—Without prejudice to any action that may be taken under the Act, any contravention of regulations 3, 4, 5 and 6 of these regulations shall constitute a violation of sub-section (2) of section 29 of the Act.

8. Redressal of grievances of Aadhaar number holders.—In the event the identity information of an Aadhaar number holder has been shared or published in a manner contrary to the provisions of the Act or regulations, the Aadhaar number holder may raise queries and grievances in accordance with the regulation 32 of the Aadhaar (Enrolment and Update) Regulations, 2016.

CHAPTER III
MISCELLANEOUS

9. Information dissemination about sharing of Aadhaar numbers.—The Authority may take necessary measures to educate Aadhaar number holders about the uses of Aadhaar numbers and implications associated with its sharing.

10. Savings.—All procedures, orders, processes, standards 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.

11. Power to issue clarifications and guidelines.—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.