THE AADHAAR (DATA SECURITY) REGULATIONS, 2016[1]

[Updated as on 15.2.2024]

In exercise of the powers conferred by clause (p) of subsection (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 makes the following Regulations, namely:—

1. Short title and commencement.—(1) These regulations may be called the Aadhaar (Data Security) 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 (18 of 2016);

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

(c) "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;

(d) "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;

(e) "information security policy" means the policy specified by the Authority under regulation 3 of these regulations;

(f) "personnel" means all officers, employees, staff and other individuals employed or engaged by the Authority or by the service providers for discharging any functions under the Act;

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

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

(i) "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;

(j) "service provider" includes all entities engaged by the Authority for discharging any function related to its processes.

---

[1] Published in the Gazette of India, Part III, Section 4, dated 14.9.2016, *vide* notification No. 13012/64/ 2016/ Legal/UIDAI (No. 4 of 2016), dated 12.9.2016.

(2) All other words and expressions used but not defined in these regulations, but defined in the Act or the Information Technology Act, 2000 and/or the rules and regulations made thereunder shall have the same meaning as respectively assigned to them in such Acts or rules or regulations or any statutory modification or re-enactment thereto, as the case may be.

3. Measures for ensuring information security.—(1) The Authority may specify an information security policy setting out inter alia the technical and organisational measures to be adopted by the Authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and Authentication Service Agencies.

(2) Such information security policy may provide for:—

(a) identifying and maintaining an inventory of assets associated with the information and information processing facilities;

(b) implementing controls to prevent and detect any loss, damage, theft or compromise of the assets;

(c) allowing only controlled access to confidential information;

(d) implementing controls to detect and protect against virus/malwares;

(e) a change management process to ensure information security is maintained during changes;

(f) a patch management process to protect information systems from vulnerabilities and security risks;

(g) a robust monitoring process to identify unusual events and patterns that could impact security and performance of information systems and a proper reporting and mitigation process;

(h) encryption of data packets containing biometrics, and enabling decryption only in secured locations;

(i) partitioning of CIDR network into zones based on risk and trust;

(j) deploying necessary technical controls for protecting CIDR network;

(k) service continuity in case of a disaster;

(l) monitoring of equipment, systems and networks;

(m) measures for fraud prevention and effective remedies in case of fraud;

(n) requirement of entering into non-disclosure agreements with the personnel;

(o) provisions for audit of internal systems and networks;

(p) restrictions on personnel relating to processes, systems and networks.

(q) inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the Authority.

(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.

***