=== Ellaquai Dehati Bank ===

EXTERNAL

Data Privacy Policy
Version 1.0
2023-24

Information Techn`ology Department
=======ELLAQUAI DEHATI BANK=======
==== 3rd Floor, Nirmaan Complex, IG Road, Barzulla, Srinagar ====
Email: mailcbs@edb.org.in

8. Data Protection

8.1 Policy Statement

8.1.1 All identified data shall be protected in all phases of its lifecycle including collection, processing, transmission, storage, exchange, and retirement. Privacy of Personally Identified Information or the Bank shall be ensured.

Standards and Procedures

8.2 Data Identification

8.2.1 Officials, designated for protection of data as per this policy, shall identify the Bank's data in following lines:

8.2.1.1 Business Data

8.2.1.1.1 Business data refers to information proprietary to the Bank which includes financials records, sales, marketing, and products data.

8.2.1.2 Personally Identifiable Information

8.1.2.1 All data which can uniquely identify an individual, either Bank's customer or employee, is called as Personally Identifiable Information (PII).

8.2.1.2.2 PII of an individual may include following but not limited to:

• Name, like full name, maiden name, mother's/father's maiden name

• Personal Identification Number like PAN, Passport Numbers, Driving License, Voter id, etc.

• Address information, e.g., residential address, office address, email address, etc.

• Contact numbers, e.g., LL/Mobile number, business or residential phone number

• Personal characteristic, e.g., photographs, fingerprints or other biometric data

• Information about an individual that is linked to one of the above like date of birth, place of birth, employment information, medical history information, financial information (credit card numbers, Bank account numbers)

8.2.1.2.3 PH which is explicitly required for a business purpose should only be collected from the individuals. All such data should be ensured for its

accuracy, authenticity, completeness, and updating on a regular basis by respective Information Owner.

AADHAAR ACT APPLICABLE CHAPTER

ENROLMENT

3

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
    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. (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) 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 (r) of sub-section (1) of section 2 of the Information Technology Act, 2000. Aadhaar number. Properties of Aadhaar number.
5. 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.

AADHAAR ACT APPLICABLE CHAPTER

6. 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. 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, require that such individual undergo authentication, or furnish proof of possession of Aadhaar number or in the case 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. (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 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.

(3) A requesting entity shall inform, in such manner as may be specified by regulations, the individual submitting his identity information for authentication, 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.

AADHAAR ACT APPLICABLE CHAPTER

(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.

9. 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. 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.ory and to perform any other functions as may be specified by regulations.

CHAPTER VI

PROTECTION OF INFORMATION

28. (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

AADHAAR ACT APPLICABLE CHAPTER

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. (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 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 Security and confidentiality of information, Restriction on sharing information.

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

(4) No Aadhaar number or core biometric information 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.

30. 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 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 (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;

(b) "electronic record" shall have the same meaning as assigned to it in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 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.

AADHAAR ACT APPLICABLE CHAPTER

31. (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. (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. (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 District Judge:

Provided that no order by the court under this sub-section shall be made without giving an opportunity of hearing to the Authority.

(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 Biometric information deemed to be sensitive Personal information.

Alteration of demographic information or biometric information.

Access to own information and records of requests for authentication.

Disclosure of information in certain cases.

records, made in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government:

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

DO's FOR AADHAAR USER AGENCIES/DEPARTMENTS

1. Read Aadhaar Act, 2016 and its Regulations carefully and ensure compliance of all the provisions of the Aadhaar Act, 2016 and its Regulations.
2. Ensure that everyone involved in Aadhaar related work is well conversant with provisions of Aadhaar Act, 2017 and its Regulations as well as processes, policies specifications, guidelines, circular etc issued by UIDAI from time to time.
3. Create internal awareness about consequences of breaches of data as per Aadhaar Act, 2016.
4. Follow the information security guidelines of UIDAI as released from time to time.
5. Full Aadhaar number display must be controlled only for the Aadhaar holder or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
6. Verify that all data capture point and information dissemination points (website, report etc) should comply with UIDAI's security requirements.
7. If agency is storing Aadhaar number in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using HSMs. If simple spreadsheets are used, it must be password protected and securely stored.
8. Access controls to data must be in place to make sure Aadhaar number along with personally identifiable demographic data is protected.
9. For Aadhaar number look up in database, either encrypt the input and then look up the record or use hashing to create Aadhaar number based index.
10. Regular audit must be conducted to ensure Aadhaar number and linked data is protected.
11. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.
12. 12.An individual in the organization must be made responsible for protecting Aadhaar linked personal data. That person should be in charge of the security of system, access control, audit, etc.
13. Identify and prevent any potential data breach or publication of personal data.
14. Ensure swift action on any breach personal data.
15. Ensure no Aadhaar data is displayed or disclosed to external agencies or unauthorized persons.
16. Informed consent - Aadhaar holder should clearly be made aware of the usage, the data being collected, and its usage. Aadhaar holder consent should be taken either on paper or electronically.
17. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure all Aadhaar holders are able to use it effectively.
18. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.
19. Create Exception handling mechanism on following lines-
20. It is expected that a small percentage of Aadhaar holders will not be able to do biometric authentication. It is necessary that a well-defined exception handling mechanism be put in place to ensure inclusion.
21. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.

22. If the schemes is family based (like PDS system), anyone in the family must be able to authenticate to avail the benefit. This ensures that even if one person is unable to do any fingerprint authentication, someone else in the family is able to authenticate. This reduces the error rate significantly.
23. If none of the above is working (multi-finger, Iris, anyone in family, etc.), then agency must allow alternate exception handling schemes using card or PIN or other means.
24. All authentication usage must follow with notifications/receipts of transactions.

DONT's FOR AADHAAR USER AGENCIE S/DEPARTMENTS

1. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc. Publication of Aadhaar details is punishable under Aadhaar act.
2. Do not store biometric information of Aadhaar holders collected for authentication.
3. Do not store any Aadhaar based data in any unprotected endpoint devices, such as PCs, laptops or smart phones or tablets or any other devices.
4. Do not print/display out personally identifiable Aadhaar data mapped with any other departmental data such as on ration card/birth certificate/caste certificate/any other certificate/document. Aadhaar number if required to be printed, Aadhaar number should be truncated or masked. Only last four digits of Aadhaar can be displayed/ printed.
5. Do not capture/store/use Aadhaar data without consent of the resident as per Aadhaar act. The purpose of use of Aadhaar information needs to be disclosed to the resident.
6. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
7. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
8. Do not permit any unauthorized people to access stored Aadhaar data
9. Do not share Authentication license key with any other entity.

ELLAQUAI DEHATI BANK
Head Office
Signed