Aadhar Data Privacy Policy

Of

Department of Posts

India

Contents

1. Introduction

i. Since Department of Posts (hereinafter referred to as “DoP”) handles Sensitive Personal Data such as the Biometric information, Aadhaar number, e-KYC information etc. of the customers, for conducting authentication with UIDAI at the time of providing the services; it becomes imperative to ensure its security and safety to prevent unauthorized access.

ii. This Policy is in line with the directions of Information Security Policy issued by UIDAI, Information Security Management Policy of DoP and is applicable wherever UIDAI information is processed and/or stored by DoP.

The following guidelines apply to all Aadhaar-related data processing.

2. Specific Purpose of Collection of Aadhar and related data

i. The identity information including Aadhaar number shall be collected for the purpose of authentication of Aadhaar number holder for cases wherever e-KYC verification is required, for a more generic purpose and broader perspective

ii. The identity information collected and processed shall only be used pursuant to applicable law and as permitted under the Aadhaar Act 2016 or its Amendment and Regulations.

iii. The identity information shall not be used beyond the mentioned purpose without consent from the Aadhaar number holder and even with consent use of such information for other purposes should be under the permissible purposes in compliance to the Aadhaar Act 2016.

iv. All personal and sensitive data collected is protected in accordance with the provisions of the Information technology Act, 2000 (“IT Act”), Digital personal Data Protection Act, 2023 (“DPDP Act”), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

3. Prohibition of Storage

DoP shall not store the data captured (both biometric and Aadhar Number) in any manner and form. Aadhaar number that are submitted by the resident / customer/ individual to the DoP and PID block *(i.e. the Personal Identity Data element which includes necessary demographic and/or biometric and/or OTP collected from the Aadhaar number holder during authentication)* hence created shall not be retained under any event and DoP shall retain the parameters received in response from UIDAI.

4. Masking of Aadhaar Numbers

Display of Full Aadhaar number of the customers shall be done only for the Aadhaar number holder or employees with special roles/users having the defined need strictly on a “need to know” basis. By default, all displays should be masked and only last four digits of the Aadhaar number shall be displayed.

5. Aadhaar Data Security

i. DoP shall implement robust security protocols, including encryption and access controls, to protect Aadhaar data in both physical and digital formats.

ii. Any security incidents affecting the confidentiality, integrity and availability of information received from the UIDAI will be reported to UIDAI at the earliest.

iii. Appropriate security and confidentiality obligations shall be implemented in the non-disclosure agreements (NDAs) with employees/contractual agencies /consultants/advisors and other personnel handling identity information.

iv. DoP shall capture the biometric information of the Aadhaar number holder using certified biometric devices as per the processes and specifications laid down by UIDAI. Only STQC certified Authentication devices shall be used to capture customers biometric information.

v. No data of the customer shall be stored within the terminal device (i.e., biometric device).

vi. The biometric details whenever captured by DoP will be used only for data exchange with UIDAI for validation purpose. A system log wherever required will be maintained to extract the details in case of disputes.

vii. The logs will capture Transaction id, timestamp etc., but will not capture / store the PID (Person Identity Data) associated with the transaction. The logs shall not, in any event, retain the PID, biometric and OTP information.

viii. Periodic Vulnerability Assessment exercise should be conducted for maintaining the security of the authentication applications. Reports shall be generated and shared upon request with UIDAI.

ix. Periodic Vulnerability Assessment (VA) exercise shall be conducted for ensuring the security of the Aadhaar infrastructure and Necessary network intrusion and prevention systems shall be implemented.

x. All hosts that handle customer's identity information shall be secured using endpoint security solutions. An anti-virus / malware detection software shall be installed on such hosts.

6. Aadhaar Authentication

i. DoP shall ensure that Aadhaar authentication requests are made only for lawful purposes, and authentication logs shall be stored only as per the timelines prescribed by the UIDAI. e-KYC shall be carried out using only biometric and/or OTP authentication modalities.

ii. Aadhaar number holder shall be provided relevant information prior to collection of identity information / personal data which include:
    a) the nature of information that will be shared by the UIDAI upon authentication;
    b) the uses to which the information received during authentication may be put;
    c) alternatives for submission of identity information.

iii. Aadhar number holder shall be notified of the authentication either through email or phone or SMS at the time of authentication.

iv. Consent of the Aadhaar number holder shall be obtained for each authentication preferably in electronic form and maintain logs of disclosure of information and records of the consent.

7. Compliance with UIDAI Guidelines

i. DoP shall comply with all guidelines issued by UIDAI from time to time, including the use of Aadhaar data for e-KYC and authentication processes.

ii. Necessary Information security trainings shall be conducted for all personnel for Aadhaar related authentication services during induction.

iii. Only licensed Authentication User Agencies (AUA), ASAs (Authentication Service Agencies) and e-KYC User Agencies (KUA) approved by UIDAI are permitted to perform Aadhaar authentication and access Authentication application, audit logs, authentication servers, application, source code, information security infrastructure. An access control list shall be maintained and regularly updated by DoP.

iv. DoP shall create internal awareness about consequences of breaches of Aadhaar data via various channels such as Newsletter articles, employee trainings, internal Memos and communications etc.

v. e-KYC information shall be stored in an encrypted form only. Such encryption shall match UIDAI encryption standards and follow the latest Industry best practice.

vi. All assets (business applications, operating systems, databases, network etc.) used for the Aadhaar authentication services shall be identified, labelled and classified.

vii. All applications used for Aadhaar authentication or e-KYC shall be tested for compliance to Aadhaar Act 2016 before being deployed in production and after every change that impacts the processing of Identity information.

viii. Identity information shall not be hosted or transferred outside the territory of India in compliance to the Aadhaar Act and its Regulations.

ix. The applications shall be audited on an annual basis by information systems auditor(s) certified by STQC, CERT-IN or any other UIDAI recognized body. The audit report shall be shared with UIDAI upon request.

8. Compliance with Data Protection laws

i. As AUA/KUA, DoP has established a data protection policy addressing, inter alia, data protection related aspects that are aligned with the Aadhaar Act, 2016 and its associated regulations and standards prescribed by UIDAI, Information Technology Act, 2000 including Information Technology (Amendment) Act 2008, the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 and Digital Personal Data Protection Act, 2023 (DPDP Act).

ii. As AUA/ KUA, DoP has published data protection policy on the website and the URL for the same is <https://www.indiapost.gov.in>

iii. Any data processing activities will be governed by principles of accountability, consent, purpose limitation, and data minimization, ensuring compliance with the DPDP Act.

iv. The Data protection policy covers aspects covering use of encryption and secure transmission protocols, regular review and audit of IT systems handling Aadhar Data to ensure compliance with reasonable security practices aligned with IT Act and IT Rules.

v. Privacy enhancing organizational and technical measures like anonymization, de-identification and minimization have been implemented to make the collection of identity information adequate, relevant, and limited to the purpose of processing.

9. Aadhaar Grievance Redressal

Any grievances related to Aadhaar data processing shall be addressed promptly. DoP's will nominate a suitable grievance officer for handling matters related to Aadhaar privacy.

10. Regulatory References

i. Aadhaar (Targeted Delivery of Financial and other Subsidies, benefits and services) Act, 2016 i.e. Aadhaar Act, 2016 and its associated regulations and standards prescribed by UIDAI
ii. Aadhar (Authentication and Offline Verification) Regulations, 2021
iii. UIDAI Information Security Policy for AUA/KUA
iv. Various circulars issued by UIDAI
v. Information Technology Act, 2000
vi. Information Technology (Amendment) Act 2008
vii. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
viii. Digital Personal Data Protection Act, 2023 (DPDP Act)