DIT- F (4)1/2008-UID-2 — 155

Department of Information Technology
Government of Himachal Pradesh
*****

From

**Principal Secretary (IT) to the
Government of Himachal Pradesh**

To

1. **All the Administrative Secretaries to the
Government of Himachal Pradesh**

2. **All Deputy Commissioners to the
Government of Himachal Pradesh**

3. **All the Heads of the Departments to the
Government of Himachal Pradesh**

Dated: Shimla-171013 the 29th May, 2017

Subject: **Data Sharing- Compliance of the IT Act 2000 and Aadhaar Act 2016.**

Sir / Madam,

I am directed to draw your kind attention to the office memorandum no: O.M. No. 10(36)/2015-EG-II (Vol-V) dated 25.03.2017 received from e-Governance Group, MeitY GOI regarding the above-cited subject (copy enclosed). The letter explains the duty of the State Government Departments to comply with IT Act 2000 and Aadhaar Act 2016. The highlighting features are as under:

1. Publishing of identity information i.e. Aadhaar number along with demographic information such as name, date of birth, address etc. is clear contravention of the provisions of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, more specifically Section 29 (2), Section 29 (3) and 29 (4) and constitutes an offence under Section 37, 40 & 41 punishable with imprisonment up to 3 years.
2. All the above sections are reproduced as under:
   a. Section 29 (2): The identity information, other than core biometric information, collected or created under this Act may be shared only in

I.T Cell

accordance with the provisions of this Act and in such manner as may be specified by regulations.

b. Section 29 (3): No identity information available with a requesting entity shall be-

    i. Used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or

    ii. Disclosed further, except with the prior consent of the individual to whom such information relates.

c. Section 29 (4): No Aadhaar number or core biometric information collected or created under this Act is respect of an Aadhaar number holder shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.

d. Section 37: Whoever, intentionally disclosed, 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 mode 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.

e. Section 40: Whoever, being a requesting entity, uses the identity information of an individual a 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 one lakh rupees or with both.

f. Section 41: Whoever, being an enrolling agency or 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 one year or with a fine which may extend to ten thousand rupees o, in the case of a company with a fine which may extend to one lakh rupees or with both.

3. Publishing of financial information including bank account details, being sensitive personal data is also in contravention of provisions under the Information Technology Act 2000 and the Rules framed thereunder, more specifically Rule 3 & Rule 6 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 and constitutes an offence under Section 43

A of the Information Technology Act 2000 and the offending parties are liable to pay damages by way of compensation to person affected.

a. The rules of Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011 are reproduced as under:

    i. Rule 3: **Sensitive personal data or information**— Sensitive personal data or information of a person means such personal information which consists of information relating to;—

        1. Password;
        2. Financial information such as Bank account or credit card or debit card or other payment instrument details ;
        3. Physical, physiological and mental health condition;
        4. Sexual orientation;
        5. Medical records and history;
        6. Biometric information;
        7. Any detail relating to the above clauses as provided to body corporate for providing service; and
        8. Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise:

    Provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules.

    ii. Rule 6: **Disclosure of information**—

        1. Disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation:

            Provided that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency shall send a request in writing to the body corporate possessing the sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

2. Notwithstanding anything contain in sub-rule (1), any sensitive personal data on Information shall be disclosed to any third party by an order under the law for the time being in force.
3. The body corporate or any person on its behalf shall not publish the sensitive personal data or information.
4. The third party receiving the sensitive personal data or information from body corporate or any person on its behalf under sub-rule (1) shall not disclose it further.

In view of the above, it is hereby informed that any act of publishing personal identity of information i.e. Aadhaar number and demographic details along with personal sensitive information such as bank details, in contravention of the Aadhaar Act, 2016 and the Information Technology Act, 2000 may be refrained with immediate effect. Further, any such content already published and still appearing publicly may be discontinues with immediate effect. Moreover, any data exchange through emails between different Government entities should be done through official email ids only using Government mail server (like NICEMAIL etc.) account. The instructions regarding "Do's and Don'ts" are attached at **Annexure "A"** for your ready reference.

Yours faithfully,

Additional Director,
Department of Information Technology
Himachal Pradesh

Annexure-"A"

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. 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.**
25. **All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, sms, physical-center, etc.).**
26. **Get all the applications using Aadhaar audited & certified for its data security by appropriate authority such as STQC/CERT-IN.**
27. **Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.**

DONT's FOR AADHAAR USER AGENCIES/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.**

Directorate of Higher Education
Himachal Pradesh

Endst. No. EDN-HE(14)-B(1)/2/2015-IT Policy Dated
Shimla-171001, the

Copy for information and necessary action to:

1. All the Deputy Directors of Higher Education with the direction to comply with **IT Act 2000 and Aadhaar Act 2016** for sharing sensitive personal data or information and disclosure of information.
2. All the Principals of Govt. Degree Colleges/Skt. Colleges/GSSSs in Himachal Pradesh with the direction to comply with **IT Act 2000 and Aadhaar Act 2016** for sharing sensitive personal data or information and disclosure of information.
3. Guard File.

Director of Higher Education
Himachal Pradesh