F.No. 4-13/2016-SS
Government of India
Ministry of Minority Affairs

11th Floor, Pt. Deendayal Antyodaya Bhawan,
C.G.O.Complex, Lodhi Road,
New Delhi-110003
Dated: 05.06.2017

To

The Principal Secretary/Secretary,
State Government/UT Administration.

Subject: Sensitization about Aadhaar and Bank Details of the beneficiaries under scholarship schemes meant for minorities

Sir,

This is with reference to the implementation of three Scholarship Schemes viz. Pre-Matric, Post Matric and Merit-cum-Means for 2016-17 of this Ministry meant for minorities.

2. In this regard, it is stated that, from the year 2015-16, all the three scholarship schemes are being implemented through the National Scholarship Portal (NSP) and Aadhaar Number, although not mandatory at present, is also being sought from the applicants. Bank details are, however to be obtained from all applicants as a mandatory field.

3. All States/UTs are requested to sensitize their respective agencies/Offices at the State/District and other levels to use sensitive information like Aadhaar Number, Bank details etc. with utmost care in conformity with provisions of Aadhaar Act, 2016 and UIDAI guidelines. A copy of guidelines dated 04.05.2017, circulated by MeitY, Government of India is enclosed for reference/compliance.

Yours faithfully

(Aditya S. Singh)
Under Secretary to the Government of India
Tel. 011-24302520

Copy to:

Nodal Officer of All States/UTs
Dealing with Minority Welfare Schemes

सत्यमेव जयते

O/o Secretary (MA)
Receipt Received on dt. 11/5/17
FTS No / Date 831/12/5/17

अरुणा सुंदरराजन, आई.ए.एस.
Aruna Sundararajan, I.A.S.

सचिव
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारत सरकार
Secretary
Ministry of Electronics &
Information Technology (MeitY)
Government of India

D.O. No. 10(13)/2017 EG-II
Dated: 4th May, 2017

Sub.: General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000.

Dear Secretary

This has reference to the OM no. 10(36)/2015-EG-II (Vol-V) dated 25.03.2017 on Data Sharing – Compliance of IT Act, 2000 and Aadhaar Act, 2016.

2. MeitY has prepared general guidelines for securing personal information and Sensitive personal information in compliance to Information Technology Act, 2000 and Aadhaar Act, 2016.

3. The aforesaid guidelines are enclosed for ensuring necessary compliance.

With regards

Yours sincerely

(Aruna Sundararajan)

To

Secretaries of all the Ministries/Departments, Government of India

इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्पलेक्स, नई दिल्ली–110003 / Electronics Niketan,6, C.G.O. Complex, New Delhi-110003
Tel. : 011-24364041 • Fax : 24363134 • email : secretary@mit.gov.in

General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000

1. Objective

The objective of this document is to assist the various government departments that collect, receive, possess, store, deal or handle (jointly referred to as "handle" or "handled" or "handling" in this document) personal information including sensitive personal information or identity information to implement the reasonable security practices and procedures and other security and privacy obligations under the IT Act 2000, section 43A (Information Technology rules, 2011 - Reasonable Security practices and procedures and sensitive personal data or information) and Aadhaar Act 2016.

2. Definitions

For the purpose of this document, the definitions as given in the IT Act 2000 and Aadhaar Act 2016 have been used. These are provided here for sake of clarity.

i. ***Personal information*** *means any information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*

ii. ***Sensitive personal data or information*** *means such personal information which consists of information relating to:*

- *Password;*
- *financial information such as Bank account or credit card or debit card or other payment instrument details;*
- *physical, physiological and mental health condition;*
- *sexual orientation;*

5.0 Basic Actions Departments should undertake should include:

5.1 Organisation Structure, Awareness and Training

i. Identify and deploy an officer responsible for security in your organization/ department
ii. 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.
iii. Ensure all officials involved in any IT related projects read Aadhaar Act, 2016 and IT Act 2000 along with its Regulations carefully and ensure compliance of all the provisions of the said Acts.
iv. Ensure that everyone including third parties involved in Digital initiatives is well conversant with provisions of IT Act 2000 and Aadhaar Act, 2016 along with its Regulations as well as processes, policies specifications, guidelines, circular etc issued by the authorities from time to time.
v. Create internal awareness about consequences of breaches of data as per IT Act 2000 and Aadhaar Act, 2016.
vi. Ensure that employees and officials understand the implications of the confidentiality and data privacy breach.

5.2 Technical and Process Controls

i. Follow the information security guidelines of MeitY and UIDAI as released from time to time.
ii. Informed consent – Ensure that the end users should clearly be made aware of the usage, the data being collected, and its usage. The user's positive consent should be taken either on paper or electronically.
iii. Ensure that any personal sensitive information such as Aadhaar Number, Bank Account details, Fund transfer details, Gender, Religion, Caste or health information display is controlled and only displayed to the data owner or various special roles/users having the need within the agency/department. Otherwise, by default, all displays should be masked.
iv. Verify that all data capture point and information dissemination points (website, report etc) should comply with IT Act and UIDAI's security requirements.

d. 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.

xvi. All access to information, or authentication usage must follow with notifications/receipts of transactions.

xvii. All agencies implementing Aadhaar authentication must provide effective grievances handling mechanism via multiple channels (website, call-center, mobile app, SMS, physical-center, etc.).

xviii. Get all the applications that collect personal sensitive information audited for application controls and compliance to the said Acts & certified for its data security by appropriate authority such as CERT-IN empanelled auditors.

xix. Use only STQC/UIDAI certified biometric devices for Aadhaar authentication.

xx. Check all IT infrastructure and ensure that no information is displayed and in case it is displayed, please remove them immediately.

xxi. Ensure that adequate contractual protection is in place in case third parties are involved in managing application/ data centers

5.3 Data Retention and Removal

i. Ensure that the department has developed a data retention policy

ii. Ensure that you do not store personal sensitive information for a period more than what is required

iii. Delete/ remove/ purge the data after a specified period

5.4 Aadhaar Specific precautions

i. Do not publish any personal identifiable data including Aadhaar in public domain/websites etc.

ii. Do not store biometric information of Aadhaar holders collected for authentication.

iii. 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.

iv. 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