भारत सरकार GOVERNMENT OF INDIA
वित्त मंत्रालय MINISTRY OF FINANCE
राजस्व विभाग DEPARTMENT OF REVENUE
प्रधान आयुक्त का कार्यालय
OFFICE OF THE PRINCIPAL COMMISSIONER
केन्द्रीय कर और केन्द्रीय उत्पाद शुल्क,
CENTRAL TAX & CENTRAL EXCISE,
कोच्चि, KOCHI
केन्द्रीय राजस्व भवन, CENTRAL REVENUE BUILDING
आई. एस. प्रेस रोड, कोच्चि, I.S. PRESS ROAD, KOCHI-682 018
E-mail: cexcochi@nic.in Fax: 0484-2390608 Phone: 0484-2390404

C.No.II/7/2/2014-Estt. Date: .07.2017

ESTABLISHMENT CIRCULAR NO. 9 /2017

Attention is invited to the following letter received from the Ministry of Finance:-

Sl. No.	Letter No. and date	Subject
1.	F.No.296/232/2015-CX-9 dated 29.05.2017	Violations of the provisions of the Aadhaar Act, 2016 and Information Technology Act, 2006

Copy of the mentioned letter may be downloaded from the website of Cochin commissionerate - www.cenexcisekochi.gov.in for information.

[C D Jose]
Assistant Commissioner [P&V]

To

1. The DC/AC of divisions under Cochin commissionerate.
2. All Section Heads in Headquarters Cochin.
3. The Superintendent (EDP) for uploading in website.
4. Notice Board, Hqrs Cochin.
5. Notice Board, Central Excise Bhavan, Kathrikadavu.

Copy to:

1. The Deputy Commissioner (CCO), Hqrs Cochin for information.

File No. 296/232/2015-CX-9
Government of India
Ministry of Finance
Department of Revenue
Central Board of Excise & Customs
*****

New Delhi, dated 29th May, 2017



To,

i) All Chief Commissioners Customs and Central Excise, Service Tax
ii) All Director General in CBEC

Subject:-Violations of the provisions of the Aadhaar Act, 2016 and Information Technology Act, 2000

Sir,

I am directed to forward herewith a copy of O.M F. No.0-21030/3/2015-Coord. dated 22.05.2017 received from Coordination Section DoR on the above mentioned subject for information and necessary action.

Yours faithfully,

Encl: As above

(V. Ganesh Kumar)
Under Secretary to the Govt. of India (CX-9)
Tel: 23092413

OSD.CXT

-2-

F.TS - 473127/17

O/o Commissioner (Coord)/CBEC
Dy/File No. ...../201
Date .....
FTS No. .....

F. No. O-21030/3/2017-Coord.
Government of India
Ministry of Finance
Department of Revenue

New Delhi, dated 22nd May, 2017

OFFICE MEMORANDUM

Subject : Violations of the provisions of the Aadhaar Act, 2016 and Information Technology Act, 2000.

The Undersigned is directed to enclose a copy of Letter File No. K-11022/642/2017-UIDAI (Auth-II) dated 4th May, 2017 received from Ministry of Electronics and Information Technology on the above mentioned subject for necessary compliance.

Encl: As Above

Narendra Kumar
22/5/17

(Narendra Kumar)
Under Secretary (Coord)
Telefax No: 23095539

Lh(EC) in mtg
Comm (Coord)

1. Chairman (CBDT)
2. Chairperson (CBEC)
3. Director, Enforcement Directorate
4. DG, CEIB
5. Director, FIU-IND
6. DS (Hqrs), Revenue Hqrs
7. DS (NC), Revenue Hqrs
8. DS (Admn), Revenue Hqrs

Copy to :

1. Commissioner (Coord. & system), CBDT
2. Commissioner (Coord.), CBEC
3. US (GAR)

US

pl. pump
26/5
SO(AS)

फाइल संख्या: No.K-11022/642/2017-UIDAI (Auth-II)
भारत सरकार
इलैक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
भारतीय विशिष्ट पहचान प्राधिकरण
अधिप्रमाणन अनुभाग

3री मंजिल, टॉवर–2, जीवन भारती भवन,
कनॉट सर्कस, नई दिल्ली–110001

दिनांक 04.05.2017

To

Secretary
Department of Revenue
Ministry of Finance
Room No. 128 A, 1st Floor,
North Block, New Delhi

DEPTT OF REVENUE
FTS 21/0841
DATE 12/5/17

Sub: Violations of the provisions of the Aadhaar Act, 2016 and Information Technology Act, 2000

Sir/Madam,

As you are aware that recently there were certain media reports regarding display of residents' Aadhaar numbers and other sensitive personal data such as bank account details etc on websites of various central and state government departments.

2. It may be noted that public display of Aadhaar numbers of residents in such a manner is violation of the section 29(4) of the Aadhaar Act, 2016. Further, financial information such as bank account details, Aadhaar number which is also being used as a financial address are sensitive personal data, the publishing of which is violation of the provisions of the Information Technology Act, 2000 and the Rules framed thereunder and constitute an offense under section 72 of the Information Technology Act, 2000. UIDAI has circulated a list of DOs and DONTs regarding usage of Aadhaar, a copy of which is enclosed for ready reference.

3. Therefore, you are requested to kindly issue instructions to the concerned that all departments need to ensure compliance with the above mentioned provisions of the Aadhaar Act, 2016 and Information Technology Act, 2000. It is also requested to provide us the list of schemes (as per the enclosed proforma) which have collected Aadhaar numbers, the format in which the beneficiary data is displayed on their respective websites and whether Aadhaar number and other sensitive personal data are published in any report / document etc.

Considering the urgency of the matter, an early reply will be appreciated.

Regards,

Yours faithfully

(Rupinder Singh)
Deputy Director General

Encl: as above

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.