

(67)

GOVT. OF NCT OF DELHI
SOCIAL WELFARE DEPARTMENT
GLNS COMPLEX, DELHI GATE, NEW DELHI-110002
[COMPUTER CELL]

F.56(320)/DSW/CC/RTI/56/2008-09/Part-1

1416-1483

dated:

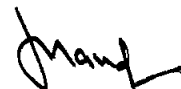
Circular

25 JUN 2020

Sub: - Security of Sensitive Personally Identifiable Information.

Please find enclosed herewith copy of a circular no. E-13014/2/2015-Development/2590-2659 dated 03-06-2020 issued by Special Secretary, Department of Information Technology, Govt. of NCT of Delhi along with a copy of letter no. 22016/08/2019-CIS.IV dated 04-05-2020 issued by Ministry of Home Affairs (CIS Division) on the subject cited above. Further, a copy of letter no. 13014/2/2015-Development/3591-3665 dated 11-09-2018 issued by Department of Information Technology, Govt. of NCT of Delhi regarding General Guidelines for securing identity information and sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000 is also enclosed.

All DDs/District Officers/HOOs/DCA/DDOs of Department of Social Welfare are requested to store, process and analyse the personally Identifiable Information like Aadhaar numbers, Mobile Numbers, password, financial information such as Bank Account or credit/debit card or other payment instrument details, photograph, finger print, iris scan etc. of Financial Assistance Schemes of citizens in a secure environment as per law and directions issued vide above mentioned circulars/ letters may be compiled with.



(Subhash Chand)

Deputy Director Admin-II

Copy for information and necessary action:-

1. All DDs/District Officers/HOOs/DCA/DDOs of Department of Social Welfare.
2. Guard File.

Encl: - As above.

GOVERNMENT OF NCT OF DELHI
DEPARTMENT OF INFORMATION TECHNOLOGY
9TH LEVEL, B-WING, DELHI SECRETARIAT, NEW DELHI-110002

No.E-13014/2/2015-Development/ 2590-2659

Dated:- 03/06/2020

CIRCULAR 06 /2020

Sub:- Security of Sensitive Personally Identifiable Information.

IT Department had vide circular dated 11.9.2018 requested all concerned to observe the rules / guidelines governing sensitive personally identifiable information. Copy of the same is available on the website ([https://it.delhi.gov.in/content/securing-identity-information-and-sensitive-personal-data?Circular%20-%20Security%20Guidelines 13.pdf](https://it.delhi.gov.in/content/securing-identity-information-and-sensitive-personal-data?Circular%20-%20Security%20Guidelines%2013.pdf)).

Ministry of Home Affairs (CIS Division) has, vide letter dated 4.5.2020 (copy enclosed as Annexure-I), asked all concerned to take steps to put in place appropriate security control and protocol for processing of Personally Identifiable Information collected in regard to containment of COVID-19, so that it is stored, processed and analysed in a secure environment as per law. The communication has also specified that such data must be destroyed as soon as the purpose, for which it was collected by authorized agency, is over. In this regard, letter No.22016/08/2019-CIS.IV dated 3rd April, 2020 (copy enclosed as Annexure-II) issued by Home Affairs, GoI may also be kindly referred for compliance.

This issues with the approval of Competent Authority.



(Ajay Chagti)
Special Secretary (IT)

To

All Addl. Chief Secretaries/ Pr. Secretaries/Secretaries/
Heads of Departments of GNCTD/Autonomous bodies/
Local Bodies of GNCTD

Encl:-As above.

24/5
Kot
Immedia

F.No. 22016/08/2019-CIS.IV
Government of India
Ministry of Home Affairs
(CIS Division)

North Block, New Delhi,
Dated: 4th May, 2020

To,

Chief Secretaries / Administrators of States/Union Territories

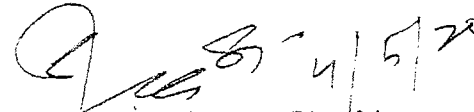
Sub: - Security of Sensitive Personally Identifiable Information

States / UTs are making efforts to contain the spread of Covid-19 inter alia by contact tracing, tracking etc. Data from various sources is being collected, collated and analyzed for this purpose. Some elements of such data falls under the category of Personally Identifiable Information (PII) and utmost precautions need to be taken for security of such sensitive data.

2. In view of above, it is requested that steps must be taken by States / UTs to put in place appropriate security control and protocol for processing of PII collected in regard to containment of Covid-19, so that it is stored, processed and analysed in a secure environment as per law. Further, such data must be destroyed as soon as the purpose, for which it was collected by authorized agency, is over.

3. In this regard, Letter No. 22016/08/2019-CIS.IV dated 3rd April, 2020, issued by Ministry of Home Affairs, may also kindly be referred for compliance (copy enclosed).

4. This has the approval of Union Home Secretary.


(Shailendra Vikram Singh)
Deputy Secretary (CIS-IV)
Tel: 23093753

Encl: As above.

Copy to: **The Directors General of Police, All States / UTs**

For information:

- I. **Secretary, Ministry of Health & Family Welfare, New Delhi**
- II. **Secretary, Department of Telecom, New Delhi**
- III. **Member Secretary, National Disaster Management Authority, New Delhi**

Immediate UB

23/4/20

F.No. 22016/08/2019-CIS.IV
Government of India
Ministry of Home Affairs
(CIS Division)

North Block, New Delhi,
Dated: 3rd April, 2020

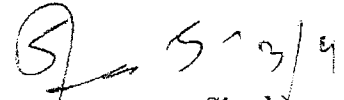
To,

Chief Secretaries of all States/UTs

Sub: - Seeking Mobile Call Records & Location Data of Telecom Subscribers- reg.

The undersigned is directed to say that it has been noticed that some States are using mobile call records and location data of telecom subscribers for the purpose of tracing of persons who have come in contact with Corona Virus infected persons.

2. It is reiterated that obtaining of such data / information is regulated under Section 5(2) of Indian Telegraph Act, 1885 and Section 69 of the Information technology Act, 2000; Rules and SOP made thereunder. All concerned are advised to ensure that the provisions of law / rules / SOP may be adhered to.
3. This has the approval of Union Home Secretary.


(Shailendra Vikram Singh)
Deputy Secretary (CIS-IV)
Tel: 23093753

Copy to:

**The Directors General of Police
All States / UTs**

For Info:

Secretary, Department of Telecom, New Delhi

14/c

Government of NCT of Delhi
Department of Information Technology
9th Level, B-Wing, Delhi Secretariat

F.No. E-13014/2/2015-Development/3591-3665 Date: - 11/09/2018

To

All Pr. Secretaries/ Secretaries/HoDs
Government of NCT of Delhi

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

Sir/Madam

I am directed to inform that it has been observed that some Departments are uploading documents containing sensitive personal information like Aadhaar numbers, Mobile Numbers, etc. on their websites. IT department has been frequently receiving warnings/communication from CERT-In regarding **Information Disclosure Vulnerability in Domain "delhi.gov.in"**.

2. All departments/agencies are therefore advised to adhere to the provisions of Aadhaar Act 2016 and Information Technology Act 2000. The "Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 framed under the IT Act are enclosed for reference (Annexure I). In this regard, 'General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000.' issued by the Ministry of Electronics and Information Technology Government of India are also enclosed for ready reference (Annexure II).

3. Departments are requested to review the contents already uploaded on their websites and remove sensitive information (if any) immediately. The



13/c

contents to be uploaded on the website must be reviewed and approved by HODs/ senior officers to ensure compliance of said Acts, Rules and

4. A confirmation letter by the Department stating that the Department's website does not contain any sensitive information may kindly be sent to IT Department latest by September 15, 2018.



(Ajay Chagti)

Spl. Secretary (IT)

Encl: Draft confirmation letter.

Copy to

1. Director General, CERT-IN, Electronic Niketan, CGO, New Delhi

12/2

Confirmation Letter

<Website> Department

It is to certify that the <website> pertaining to <department> has no sensitive information as per the Aadhaar Act 2016 and Information Technology Act 2000. The guideline issued by the Ministry of Electronics and Information Technology Government of India has been complied with.

<Signature of Head of Office>

<date>

or encryption or decryption keys that one uses to gain admittance or access to information;

- (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.

(2) All other words and expressions used and not defined in these rules but defined in the Act shall have the meanings respectively assigned to them in the Act.

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

- (i) password;
- (ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;
- (iii) physical, physiological and mental health condition;
- (iv) sexual orientation;
- (v) medical records and history;
- (vi) Biometric information;
- (vii) any detail relating to the above clauses as provided to body corporate for providing service; and
- (viii) 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.

4. **Body corporate to provide policy for privacy and disclosure of information.**— (1) The body corporate or any person who on behalf of body corporate collects, receives, possess, stores, deals or handle information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who has provided such information under lawful contract. Such policy shall be published on website of body corporate or any person on its behalf and shall provide for—

- (i) Clear and easily accessible statements of its practices and policies;
- (ii) type of personal or sensitive personal data or information collected under rule 3;

MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
(Department of Information Technology)
NOTIFICATION
New Delhi, the 11th April, 2011

G.S.R. 313(E).—In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government hereby makes the following rules, namely:--

1. **Short title and commencement** — (1) These rules may be called the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.
(2) They shall come into force on the date of their publication in the Official Gazette.
2. **Definitions** — (1) In these rules, unless the context otherwise requires,--
 - (a) "Act" means the Information Technology Act, 2000 (21 of 2000);
 - (b) "Biometrics" means the technologies that measure and analyse human body characteristics, such as 'fingerprints', 'eye retinas and irises', 'voice patterns', 'facial patterns', 'hand measurements' and 'DNA' for authentication purposes;
 - (c) "Body corporate" means the body corporate as defined in clause (i) of explanation to section 43A of the Act;
 - (d) "Cyber incidents" means any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation;
 - (e) "Data" means data as defined in clause (o) of sub-section (1) of section 2 of the Act;
 - (f) "Information" means information as defined in clause (v) of sub-section (1) of section 2 of the Act;
 - (g) "Intermediary" means an intermediary as defined in clause (w) of sub-section (1) of section 2 of the Act;

behalf of such body corporate.

(7) Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing his consent, the body corporate shall have the option not to provide goods or services for which the said information was sought.

(8) Body corporate or any person on its behalf shall keep the information secure as provided in rule 8.

(9) Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month from the date of receipt of grievance.

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 or information shall be disclosed to any third party by an order under the law for the time being in force.

- (iv) disclosure of information including sensitive personal data or information as provided in rule 6;
- (v) reasonable security practices and procedures as provided under rule 8.

5. Collection of information.— (1) Body corporate or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

(2) Body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

- (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
- (b) the collection of the sensitive personal data or information is considered necessary for that purpose.

(3) While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

- (a) the fact that the information is being collected;
- (b) the purpose for which the information is being collected;
- (c) the intended recipients of the information; and
- (d) the name and address of —
- (i) the agency that is collecting the information; and
- (ii) the agency that will retain the information.

(4) Body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.

(5) The information collected shall be used for the purpose for which it has been collected.

(6) Body corporate or any person on its behalf permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient shall be corrected or amended as feasible:

Provided that a body corporate shall not be responsible for the authenticity of the personal information or sensitive personal data or information supplied by

3/c

(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.

7. Transfer of information.-A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules. The transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

8. Reasonable Security Practices and Procedures.— (1) A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.

(2) The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard referred to in sub-rule (1).

(3) Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

(4) The body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

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/c

Ministry of Electronics and Information Technology
Government of India

- *medical records and history;*
- *biometric information*

iii. *Identity information in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information; wherein **biometric information** means photograph, finger print, Iris scan, or such other biological attributes of an individual; and **demographic information** includes information relating to the name, date of birth, address and other relevant information of an individual.*

3. Document structure

This document is structured to provide general guidelines to various Government departments that are handling Personal information or sensitive personal data or information as per the IT Act 2000, section 43 A and Aadhaar Act 2016.

4. Intended audience

The intended audience for this document from the various government departments that are handling personal information or sensitive personal data or information or identity information as defined above are provided as follows:

- i. Information Technology department or division or function
- ii. Technology department or division or function
- iii. Legal department or division or function
- iv. Information security department or division or function
- v. Chief Information Security officer
- vi. Chief Technology officer
- vii. Chief Information Technology officer

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.

3/c

Ministry of Electronics and Information Technology
Government of India

- v. If agency is storing Aadhaar number or Sensitive personal information in database, data must be encrypted and stored. Encryption keys must be protected securely, preferably using Hardware Security Modules (HSMs). If simple spreadsheets are used, it must be password protected and securely stored.
- vi. Access controls to data must be in place to make sure sensitive personal information including Aadhaar number and demographic data is protected.
- vii. 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.
- viii. Regular audit must be conducted to ensure the effectiveness of data protection in place.
- ix. Identify and prevent any potential data breach or publication of personal data.
- x. Ensure swift action on any breach of personal data.
- xi. Ensure that the system generates adequate audit logs to detect any breaches
- xii. Ensure no sensitive personal data is displayed or disclosed to external agencies or unauthorized persons.
- xiii. Authentication choice - When doing authentication, agency should provide multiple ways to authenticate (fingerprint, iris, OTP) to ensure that all Aadhaar holders are able to use it effectively.
- xiv. Multi-factor for high security - When doing high value transactions, multi-factor authentication must be considered.
- xv. In case department is using Aadhaar Authentication, it should follow exception handling mechanism on following lines-
 - a. 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.
 - b. If fingerprint is not working at all even after using multi-finger authentication, then alternate such as Iris or OTP must be provided.
 - c. 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.

2/c

Ministry of Electronics and Information Technology
Government of India

- 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

1/c

Ministry of Electronics and Information Technology
Government of India

- number if required to be printed. should be truncated or masked. Only last four digits of Aadhaar can be displayed/printed
- v. 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
 - vi. Do not disclose any Aadhaar related information to any external/unauthorized agency or individual or entity.
 - vii. Do not locate servers or other IT storage system/ devices having Aadhaar data outside of a locked, fully secured and access-controlled room
 - viii. Do not permit any unauthorized people to access stored Aadhaar data
 - ix. Do not share Authentication license key with any other entity.
