**GOVERNMENT OF NCT OF DELHI**
**PUBLIC WORKS DEPARTMENT**
**5TH LEVEL "B" WING**
**DELHI SECRETARIAT: NEW DELHI**

No.F.10(6)/ PWD-I/Misc./2016/Vol-IV/ 12840

Dated: 18/09/18

प्रमुख अभियन्ता
आवती सं. 11588
दिनांक 19/9/18
प्रमुख अभियन्ता (I)-1
निदेशक (कार्य एवं स्था.)
निदेशक (अनुरक्षण)
उप सतर्कता अधिकारी
उपनिदेशक (कार्य/स्था/अनु/सत.)

To,

The Engineer-in-Chief,
Public Works Department
Govt. of NCT of Delhi
MSO Building, IP Estate
New Delhi-110002

**Sub: Forwarding of letters/orders/Circulars.**

Sir,

Please find enclosed herewith the copy of the following letters/circular/orders etc. with necessary action as mentioned against them.

| Sl. No. | PUC No. and Subject | Remarks |
|---|---|---|
| 1. | Letter No.F.01/18/2005/DOV/14578-14581/2247 dated 06/09/2018 received from Dy. Secretary (Vigilance), GNCTD, regarding forwarding of CVC Circulars. | For information and compliance. |
| 2. | F. No. E-13014/2/2015-Development/3591-3665 dated 11/09/2018 received from Spl. Secretary (IT), Department of Information Technology, GNCTD, regarding General Guidelines for securing Identity information and Sensitive personal data or information in compliance to Aadhaar Act, 2016 and Information Technology Act, 2000. | For information and necessary action. |
| 3. | Office order issued vide F.No. 2/559/2018/CT-III/GAD/9023 dated 10.09.2018 received from Spl. Secretary (GAD), Caretaking Branch GNCTD, regarding stopping the misuse of Govt./Govt. Hired Pvt. Vehicles | For information and compliance and ATR may be submitted. |
| 4. | U.O. letter No. minhealth/2018/7777-7792 dated 11/09/2018 received from Secretary to Minister, PWD, regarding foreign visit of a delegation led by Hon'ble CM to Seoul (South Korea) from September 11-15-2018. | For information. |
| 5. | Advisory issued vide no. JLC/CLA/011/Lab/2705 dated 07/09/2018 received from Addl. Labour Commissioner, O/o The Secretary cum Labour Commissioner GNCTD regarding deployment of contract Labour through outsource agencies in various departments of GNCTD and other related issues, problems associated with contract Labour. | For information and compliance. |

Yours Sincerely,

**(L.R. MEENA)**
**Deputy Secretary (PWD/ADMN)**

**Encl: As above.**

AD(m-2) 24/9
AD(Vig.)
GA

कार्यालय प्रमुख अभियन्ता लो० नि० वि०
सं० ई-इन-ची/पी/जनुल/2018/6041(H) दि० 26/09/2018
प्रतिलिपि-सूचना एवं आवश्यक कार्यवाही हेतु प्रेषित।
1. लो० नि० वि० की वेब-साईट।

सहायक प्रशासनिक अधिकारी
कार्यालय प्रमुख अभियंता
लो० नि० वि०, दिल्ली सरकार
12वां तल, पुलिस मुख्यालय,
26 नई दिल्ली-110002

Circular

GOVERNMENT OF NATIONAL CAPITAL TERRITORY OF DELHI

**{DIRECTORATE OF VIGILANCE}**

LEVEL-4 : C- WING: DELHI SECRETARIAT: NEW DELHI-110002

*(Phone No. 23392257 & Fax No. 23392354/23392353)*

No.F.01/18/2005/DOV/ 14578-14581 2247 Dated: 6/9/18

To

The Pr. Secretary/Secretary/Head of Department(s),
All Departments under Govt. of NCT of Delhi,
New Delhi/Delhi.

PWD SECRETARIAT
Govt. of NCT of Delhi
5th Level, 'B' Wing
Dy No. Vig/2018/13887
Date 11/09/2018

**Subject: Forwarding of CVC Circulars – regarding.**

Sir/Madam

I am directed to forward herewith the following circulars, as received from Central Vigilance Commission, Satarkta Bhawan, GPO Complex, INA, New Delhi-23 on the subject cited above, for its compliance please.

| Sl. No. | Circular No. (with endorsement No. and date) | Subject of the Circular |
|---|---|---|
| 01. | Circular No.07/07/18 (Endorsement No.000/VGL/18-388880 dated 26/07/2018) | Adherence to time limits in processing of disciplinary cases – regarding. |
| 02. | Circular No.09/07/18 (Endorsement No.018/VGL/044-390291 dated 27/07/2018) | CVO to closely monitor presentation of case by Presenting Officer before the IO. |
| 03. | Circular No.08/07/2018 (Endorsement No.99/VGL/087-389176 dated 31/07/2018) | Simultaneous action of prosecution and initiation of departmental proceedings – guidance thereof. |

SS(PWD) — on leave
DS(Vig)
SO(Vig) 13.9.18

Yours faithfully,

06/9/18

(K.S. MEENA)
DEPUTY SECRETARY (VIGILANCE)

***Encl : As above.***

13/9

No.F.01/18/2005/DOV/ 14578-14581 Dated: 6/9/18

**Copy forwarded for information to:-**

1. The Director, Central Vigilance Commission, Satarkta Bhawan, G.P.O. Complex, Block-A, INA, New Delhi-110023.
2. PA to Office of IA's with the request to bring the contents of the above referred circulars into the knowledge of Inquiring Authorities of DOV.
3. The Assistant Directors/Section Officers (dealing with DP Seats), Dte of Vigilance, GNCTD with the request to ascertain the requisite reports from the Presenting Officers in terms of Circular No.09/07/18 and submit each and every report, so received from PO's, to the Secretary (Vigilance) in compiled manner.
4. Guard File/Consultant, Dte of Vigilance, GNCT of Delhi.

14/9

06/9/18

(K.S. MEENA)
DEPUTY SECRETARY (VIGILANCE)

E Address :
TA: New Delhi
Address
gil@nic.in
ebsite
www.cvc.nic.in
EPABX
on 24600200
फैक्स / Fax : 24651186

Directorate of Vigilance
Dy. No. 13002
Date 24/08/18
Govt. of NCT of Delhi

Delhi Sachivalaya
R&I Br.
Govt. of NCT of Delhi
23 AUG 2018
Dy. No. CAD/2018/39913

सत्यमेव जयते

केन्द्रीय सतर्कता आयोग
CENTRAL VIGILANCE COMMISSION

सतर्कता भवन, जी.पी.ओ. कॉम्पलैक्स,
ब्लॉक–ए, आई.एन.ए., नई दिल्ली–110023
Satarkta Bhawan, G.P.O. Complex,
Block A, INA, New Delhi-110023

OFFICE OF THE CHIEF SECRETARY
GOVT. OF NCT OF DELHI
23 AUG 2018

सं./No. 000/VGL/18-3888

दिनांक / Dated 26.07.2018

Circular No.07/07/18

**Subject: Adherence to time limits in processing of disciplinary cases – reg.**

**Reference: (i) Commission's Letter No.000/VGL/18 dated 23.05.2000**
**(ii) Commission's Office Order No.51/08/2004 dated 10.08.2004**
**(iii) Commission's Circular No.02/01/2016 dated 18.01.2016**

The Commission has been emphasizing from time to time on the need for expeditious completion of disciplinary proceedings. The model time limits for investigation of complaints and for different processes of disciplinary proceedings have been laid down in Commission's letter of even number dated 23rd May 2000.

2. The Commission would like to invite the attention of the Administrative Authorities /Disciplinary Authorities to the undue delays in finalizing vigilance cases especially the conduct of disciplinary proceedings despite having a built in time line for every activity. Further, such unexplained delays lead to Central Administrative Tribunals and the High Courts quashing the charge-sheet(s) on the sole ground that the concerned Disciplinary Authorities had issued charge-sheets to the delinquents after very long periods of commission of alleged misconduct etc. and also for unexplained delays in conducting disciplinary inquiries.

3. Timely completion and finalization of disciplinary proceedings is the prime responsibility of the Disciplinary Authority/Administrative Authorities concerned in all Departments/ Organizations. More so, such long delays in finalizing disciplinary matters are not only unjust to officials who may be finally exonerated, but helps the guilty to evade punitive action. The Commission had earlier vide its circular no.02/01/2016 dated 18/01/2016 emphasized on the various steps needed to be taken by all concerned obviating delays at different stages of the process right from investigation to finalization of disciplinary proceedings by way of regular monitoring of these cases/matters.

4. The Commission while reiterating the above said instructions would impress upon all concerned that the time limits prescribed by the Commission/DoPT for processing disciplinary cases at various stages may be strictly adhered to. All disciplinary authorities in each Ministry/Department/Organization need to regularly monitor the progress of individual disciplinary cases and take necessary steps as deemed appropriate to ensure that the disciplinary proceedings are completed within prescribed time-limits and are not unduly delayed.

5. All CVOs are also therefore advised to apprise the concerned officers regarding the above guidelines for compliance in monitoring progress/ handling disciplinary proceedings.

Ahmad

(M.A. Khan)
Officer on Special Duty

To

(i) The Secretaries of all Ministries/Departments of GoI.
(ii) All Chief Executives of CPSUs/PSBs/FIs/PSICs/Autonomous Bodies/etc.
(iii) All CVOs of Ministries/Deptts/CPSUs/PSBs/FIs/PSICs/Autonomous Organizations.
(iv) Website of CVC

136/C

Telegraphic Address :
"SATARKTA: New Delhi

E-Mail Address
cenvigil@nic.in

Website
www.cvc.nic.in

EPABX
24600200

फैक्स / Fax : 24651186

is on leave

Directorate of Vigilance
Govt. of NCT of Delhi
Dy. No. 13000
24/08/18
Date

सत्यमेव जयते

OFFICE OF THE CHIEF SECRETARY
GOVT. OF NCT OF DELHI
23 AUG 2018

केन्द्रीय सतर्कता आयोग
CENTRAL VIGILANCE COMMISSION

केन्द्रीय सतर्कता आयोग
CENTRAL VIGILANCE COMMISSION
Govt. of NCT of Delhi
Dy. No. CAD/2018/39990

सतर्कता भवन, जी.पी.ओ. कॉम्पलैक्स,
ब्लॉक-ए, आई.एन.ए., नई दिल्ली-110023
Satarkta Bhawan, G.P.O. Complex,
Block A, INA, New Delhi-110023

स. / No. 018/VGL/044-3902

दिनांक / Dated 27.07.2018

Secy(Vig)
SCV
PA circulate
24/8/18
SS(Vig)
PA(Vig)

Also seek reports of POs.

Circular No. 09/07/18

**Subject: CVO to closely monitor presentation of case by Presenting Officer before the IO**

It has been noticed by the Commission that many of the CVOs are not monitoring the presentation of cases by the Presenting Officers (PO) before the Inquiry Officers (IO). Undesirable practice of POs taking decisions contrary to the position stated in the charge-sheet without the specific consent of the Disciplinary Authority has also been noticed.

2. In this regard attention is invited to para 7.24.3 (xi) of Vigilance Manual 2017 whereby the Presenting Officers are required to keep the Disciplinary Authority posted with the progress of inquiry proceedings by sending a brief of work done at the end of each hearing. Attention is also invited to para 17 of Chapter 15 of the Handbook for Inquiry Officers and Disciplinary Authorities issued by ISTM (DoPT) wherein guidelines on the responsibilities of the PO during the Regular Hearing have been described in detail.

3. The Presenting Officer is required to lead the evidence of the prosecution logically and forcefully before the Inquiring Authority. The CVOs are required to monitor the progress of inquiry proceedings including the quality of performance of Presenting Officers before the IO on a regular basis and keep the disciplinary authorities posted about it. While examining some of the cases referred to the Commission for second

SS(Vig)
24/8/18
DS(Vig)
28/8/18
AD I
SO(A)
28/8/18
24/8/18

Contd/..

stage advice, it has been noticed by the Commission that some of the Presenting Officers (POs) have taken a stand / position contrary to the stand / position stated in the charge-sheet without the explicit consent of the Disciplinary Authority. In some cases, the POs have not presentedsome of the listed/ relied upon documents. Further, in some cases, the POs have not even ensured that the listed witnesses are summoned and produced before the Inquiring Authority for examination and substantiating the position stated in the charge-sheet. There are also instances where the POs have not sought additional documents to be produced before the IO even though they were felt essential for sustaining the charges/imputations.

4. The Commission conveys that the CVOs do not become *functus officio* once the PO is appointed ina departmental proceeding.The CVOs need to closely monitor the presentation of the case by the PO before the IO. The Commission would therefore advise all CVOs to closely monitor the presentation of cases made by the Presenting Officers before the Inquiring Authority and ensure that the cases are suitably presented before the IO on behalf of the Disciplinary Authority.The performance of the CVOs in this regard will be closely watched by the Commission. Further, for any of the observations in the conduct of the proceedings the CVO is answerable.

5. This issues with the approval of the Commission.

(M. A. Khan)
Officer on Special Duty

To

1. All CVOs of Ministries/Departments/CPSEs/PSBs/FIs/PSICs/Autonomous Organisations

2. NIC for uploading the circular on CVC's website

Website
www.cvc.nic.in
EPABX
24600200
फैक्स / Fax : 24651186

So tcs

Director of Vigilance
Dy. No. 13961
Date 24/08/18
Govt. of NCT of Delhi

OFFICE OF THE CHIEF SECRETARY
GOVT. OF NCT OF DELHI
23 AUG 2018
Dy. No.

केन्द्रीय सतर्कता आयोग
CENTRAL VIGILANCE COMMISSION
Dy. No. CAD/2018/39991

सतर्कता भवन, जी.पी.ओ. कॉम्प्लैक्स,
ब्लॉक–ए, आई.एन.ए., नई दिल्ली–110023
Satarkta Bhawan, G.P.O. Complex,
Block A, INA, New Delhi-110023

स / No. 99/VGL/087-389176

दिनांक / Date 31st July 2018

Circular No.08/07/2018

23/8/18

Subject: **Simultaneous action of prosecution and initiation of departmental proceedings – guidance thereof.**

Secy(Vig)
SCV
Pl. circulate
Sd/- 24/8/18

As per judgements of the Hon'ble Supreme Court and guidelines of Department of Personnel & Training issued thereon, it has been reaffirmed that there is no bar in conducting simultaneous criminal and departmental proceedings. Attention is invited to the Department of Personnel & Training O.M. No 11012/6/2007-Estt.(A-III) dated 1st August, 2007 and 21st July 2016 in this regard

2. The Commission while examining the disciplinary cases referred to it for advice has noticed that in cases where simultaneous action of prosecution and initiation of departmental proceedings are advised, the departmental proceedings are unduly delayed by Departments/Organisations by keeping them in abeyance on the ground that the matter is under trial in the Court. Such an approach in finalizing disciplinary matters is a matter of serious concern and is also not a correct approach.

DS(Vigg)
24/8/18

3. The Disciplinary Authority has been vested with the powers to carry out its statutory duty / obligations by initiation of appropriate departmental actions. This is as much to ensure that a delinquent public servant does not get undue benefit either by the long pendency of court proceedings or by the higher standard of proof required as it is to protect innocent public servant from vexatious proceedings. It is not open to the Disciplinary Authorities to await the outcome or decision of investigating / prosecuting agency or the Court trial.

DS(Vig.)
28/8/18
AD-I
Putup
SO(A)
28/8/18

4 The Commission would like to clarify that Disciplinary Authorities are vested with responsibility to ensure that employees under their control against whom criminal trial is pending are proceeded against forthwith for simultaneous departmental proceedings. Further, a view as to whether simultaneous disciplinary proceedings are to be initiated need to be invariably taken by the Competent Authorities at the time of considering the request for grant of sanction for prosecution

itself However, the Disciplinary Authority may withhold departmental proceedings only in exceptional cases wherein the charge in the criminal trial is of grave nature which involves questions of fact and law. In other words, in complex matters where, in case it is not possible to delineate the misconduct for the purpose of RDA. If the charge in the criminal case is of a grave nature which involves complicated questions of law and fact, it would be desirable to stay the departmental proceedings till the conclusion of the criminal case. Further, even if stayed at one stage, the decision may require reconsideration, if the criminal case gets unduly delayed. It may be noteworthy to mention that the Hon'ble Supreme Court in State of Rajasthan vs. B.K.Meena & Ors (1996) 6 SCC 417 emphasised the need for initiating departmental proceedings and stated as below:

"It must be remembered that interests of administration demand that the undesirable elements are thrown out and any charge of misdemeanor is enquired into promptly. The disciplinary proceedings are meant not really to punish the guilty but to keep the administrative machinery unsullied by getting rid of bad elements. The interest of the delinquent officer also lies in a prompt conclusion of the disciplinary proceedings. If he is not guilty of the charges, his honour should be vindicated at the earliest possible moment and if he is guilty, he should be dealt with promptly according to law. It is not also in the interest of administration that persons accused of serious misdemeanor should be continued in office indefinitely, i.e., for long periods awaiting the result of criminal proceedings."

5. The Commission would, therefore, advise all concerned Administrative Authorities that in cases where it is appropriate to initiate disciplinary proceedings along with criminal prosecution, the disciplinary proceedings must be initiated simultaneously

6. All Ministries/Departments/Organisations may apprise the above guidelines to the concerned officers for compliance in cases of simultaneous proceedings.

(M.A. Khan)
**Officer on Special Duty**

To

(i) The Secretaries of all Ministries/Departments of GoI.
(ii) All Chief Executives of CPSUs/PSBs/FIs/PSICs/Autonomous Bodies/etc
(iii) All CVOs of Ministries/Departments/CPSUs/PSBs/FIs/PSICs/Autonomous Organizations.
(iv) Website of CVC

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

PWD SECRETARIAT
Govt. of NCT of Delhi
Dy No. PWD/2018/23817
Date 12/09/2018

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

SS(PWD) – On leave DS(Admn) 13.9.18 SO (Admn)

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').

14/9

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

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

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

## Confirmation Letter

<Name of 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 guidelines issued by the Ministry of Electronics and Information Technology Government of India has been complied with.

<Signature of Head of Office>
<date>

(h) "Password" means a secret word or phrase or code or passcode or secret key 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 on 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 snail 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) 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 cut 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;*



2 of 6

- *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.

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.

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

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.

yii. 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.

**********

PWD/2018/23774
12/09/2018

MOST IMMEDIATE
TIME BOUND

GOVERNMENT OF N.C.T. OF DELHI
GENERAL ADMINISTRATION DEPARTMENT
(CARETAKING BRANCH), 2ND LEVEL, A-WING
DELHI SECRETARIAT, I.P. ESTATE, NEW DELHI-02

F. 2/559/ 2018/ CT-III/GAD/ 9023 Dated: 10.09.2018

## OFFICE ORDER

In continuation to this office Order No 8954 dt.24.08.2018 for stopping the misuse of Government / Government hired private vehicles, I am directed to convey that the competent authority has expressed his displeasure for non-compliance of the guidelines therein, within stipulated time frame. Hon'ble Chief Minister has further appointed Addl. Chief Secretary (GAD) to coordinate and monitor the said exercise in whole of GNCTD (including all Corporations) to ensure

(i) All vehicles have GPS in place before 30th September'18.
(ii) No payment for diesel / petrol / rent of any vehicles shall be made from 1st October'18 which are without GPS.

It shall be the responsibility of the respective HOD / Secretary / Senior most Officer of the Department / Corporation / Board / all other Government agencies to ensure strict implementation of the directions indicated in Orders dated.24.4.2018 & as above and forward the compliance to this office. Further, a certificate as per proforma attached be submitted by each officer to their respective HODs/Secretaries and consolidated compliance report be forwarded to GAD on or before 1.10.2018.

No further extension of time shall be granted.

(J.P. Agrawal)
Spl. Secy. (GAD)

SS(PWD)
DS(Admn)PWD

F. 2/559/ 2018/ CT-III/GAD/ 9023 Dated. 10.09.2018

Copy forwarded for information and necessary action to:-

1. Principal Secretary to Lt. Governor, Delhi.
2. Additional Secretary to Chief Minister, Govt. of NCT of Delhi.
3. Secretary to Speaker, Delhi Vidhan Sabha, Delhi.
4. Secretary to Dy Chief Minister, Govt. of NCT of Delhi.
5. Secretaries to all Ministers, Govt. of NCT of Delhi.
6. All Addl. Chief Secretaries/ Pr.Secretaries / Secretaries/ HOD's, Govt. of NCT of Delhi.
7. Principal Secretary (Finance), GNCTD for information and appropriate action.
8. OSD to Chief Secretary, Govt. of NCT of Delhi.
9. All HODs / Local Bodies / Public Undertakings/Autonomous Bodies/Universities/ Institutions/Commissions, Govt. of NCT of Delhi.
10. Secretary, Legislative Assembly Secretariat, Govt. of NCT of Delhi.

13/9
SO(Admn)
13.9.18
14/9
Ms. Arora

(J.P. Agrawal)
Spl. Secy. (GAD)

## CERTIFICATE
(To be individually signed by all the Officers)

In compliance to Office Order No.F.2/559/ 2018/ CT-III/GAD/8954 dated.24.08.2018 issued by GAD, I, _____, Designation _____, _____, working in _____ Department, do hereby confirm that only one vehicle No. _____ of _____ (make), provided by _____ Department is being used by me for official purpose.

No other vehicle of the any department is being used by the undersigned. I am also not claiming Transport Allowance.

Dated:

_ _ _ _ _ _ _ _ _ _ _

(Signature)

Name_____

Designation_____

Department_____

**OFFICE OF MINISTER OF HEALTH,**
**POWER, PWD, HOME, UD, I&FC & INDUSTRIES**
GOVT. OF DELHI: DELHI SECRETARIAT
ROOM NO.704: 7TH LEVEL : 'A' WING
I.P. ESTATE: NEW DELHI
**********

**Sub:- Foreign visit of a delegation led by Hon'ble CM to Seoul (South Korea) from September 11-15, 2018.**

Shri Satyendar Kumar Jain, Hon'ble Minister of Health, Home, Power, PWD, UD, I&FC & Industries, Govt. of NCT of Delhi and the undersigned will be visiting Seoul (South Korea) as members of a delegation led by Hon'ble CM, Delhi from September 11-15, 2018 for signing of Twinning Agreement between GNCT of Delhi and Seoul Metropolitan Government (SMG) as per following schedule:-

**Departure**

| | | | |
|---|---|---|---|
| 11.09.2018 | Dep. | New Delhi | 1940 hrs. by Flight No.KE 482 |
| | Arr. | Incheon Seoul | 0640 hrs. (Korean Airlines) |

**Arrival**

| | | | |
|---|---|---|---|
| 15.09.2018 | Dep. | Seoul | 1335 hrs. by Flight No.KE481 |
| | Arr. | New Delhi | 1805 hrs. (Korean Airlines) |

11/9/18

**(G. SUDHAKAR)**
**Secretary to Minister of**
**Health, Power, PWD, Home, UD, I&FC & Industries**
**Ph.No.23392116/23392117**

**U.O. No. minhealth/2018/** 7777-7792 **Dated:** 11/09/2018

Copy for information to:-

1. Pr. Secretary to L.G.
2. Spl. Secretary to C.M.
3. Secretary to Dy. CM/Labour/Transport/Food & Supply/Social Welfare
4. S.O. to Chief Secretary
5. ACS(Home)/ACS (PWD)/Pr. Secretary (UD)/Pr. Secretary-cum-Commissioner (Industries)/ Secretary (I&FC)/Secretary (Power)/ Secretary (H&FW)

**OFFICE OF THE SECRETARY-CUM-LABOUR COMMISSIONER**
**GOVT. OF NCT OF DELHI**
**5, SHAM NATH MARG, DELHI-110054**

No. JLC/CLA/011/CAS/2705

Dated: 7/9/2018

PWD SECRETARIAT
C
Dy No. PWD/2018/23801
Date 12/09/2018

# ADVISORY

Contract Labour Advisory Board constituted under the provisions of Contract Labour (R &A) Act, 1970 was notified vide notification No.2275 dated 14.11.2017, this is a tripartite statutory board and is headed by Hon'ble MoL, GNCTD as its chairman. The said board has been discussing various issues regarding deployment of contract labour through various outsourced agencies in various departments of Govt. of NCT of Delhi and other related issues/problems associated with contract labour.

E-in-C

A meeting with central trade union representatives was convened on 21.08.2018 under the chairmanship of Hon'ble MoL, GNCTD wherein among other issues it was resolved that based on the recommendation of Contract Labour Advisory Board, no contractor-outsourced agency who has deployed workers in any department of Govt. of Delhi shall terminate the services of workers till decision for keeping such workers on the roll of Govt. department is taken.

SO(Admn) 13.9.18

Accordingly, Heads of various departments are requested to bring this advisory to the notice and knowledge of respective outsourced agencies /contractors and also ensure compliance of the same.

7/9/18

(Dr. Rajender Dhar)
Addl.Labour Commissioner

SS(PWD)
PS(Admn)/PWD

Copy to:- 13/9

1. All Principal Secretaries/Secretaries/HODs of Delhi Govt. Departments.
2. Secretary to Hon'ble MoL for information.

14/9
Ms. Anuj