GURU GOBIND SINGH INDRAPRASTHA UNIVERSITY

Guru Gobind Singh Indraprastha University

(A State University established by the Government of NCT of Delhi)
Sector 16-C, Dwarka, New Delhi 110078

University IT Services Cell

[Room No. D-412, Phone: 011-25302746, Email: uits@ipu.ac.in]

Ref: GGSIPU/UITS/ 571 Date: 20-09-2023

CIRCULAR

An email received through Office of Registrar from Joint Director (IT), Dept. of IT, Govt of NCT of Delhi regarding sensitive personal information in compliance to Aadhar Act 2016 and IT Act, 2000.

The same is attached with this circular as the ready reference.

All employees and students of University are requested to follow the above laid guidelines.

Prof. Pravin Chandra
(Incharge, UITS)
University IT Services
GGS Indraprastha University
Sector-16C, Dwarka
New Delhi-110078

Copy for information & compliance of circular to:-

1. All Deans, Directors and Branch Heads, GGS Indraprastha University
2. AR to Vice Chancellor - For Kind Information to the Hon'ble Vice Chancellor
3. AR to Registrar - For Kind Information to worthy Registrar
4. UITS – To upload on University
5. Guard File

20/09/2023

Pushpendra K. Mishra
(System Administrator, UITS)

281 C

Government of NCT of Delhi
Department of Information Technology
9th Level, B wing Delhi Secretariat IP Estate, New Delhi
https://it.delhi.gov.in

F.17/2/2019-Dir(DeGS)/Secy(IT)/CD-93058/5771-5850 dated 01/09/2023

Circular

May please refer to general guidelines issued vide *F.No. E-13014/2/2015-Development/3591-3665 dated 11.09.2018* by IT Department, GNCTD, on securing identity and Sensitive personal data information in compliance to Aadhar Act, 2016 and IT Act, 2000 (*Copy Enclosed*)

2. In this regard, it has been observed that some departments are still having sensitive personal information like Aadhar numbers, PAN details, Mobile numbers etc. on their websites. IT Department has been receiving complaints/communications on this matter.

3. All departments are therefore, once again, advised to adhere to the provisions of Aadhar Act 2016, Information Technology Act 2000 & its subsequent amendments and new Data Policy 2023 *(The Digital Data Protection Act, 2023)*.

4. Also, Departments are requested to check/review the contents already uploaded in their websites and remove sensitive information, if any, immediately. The contents to be uploaded on the websites including Centralized circular/order/Important Schemes etc. must be reviewed and approved by HOD/Senior Officers to ensure compliance of said Acts, Rules and Provisions.

5. This issues with the prior approval of the Secretary (IT).

Santulan

(Santulan Chaubey)
Joint Director (IT)

Copy to:

All Addl. Chief Secretaries/Pr. Secretaries/Secretaries/ Head of Local /Autonomous Bodies, GNCTD

F.17/2/2019-Dir (DeGS)/Secy (IT)/CD-93058/5771-5850 dated 01/09/2023

Copy for information to:

1. Staff Officer to Chief Secretary, Delhi Secretariat, GNCTD
2. PS to Secretary to Hon'be L.G., Raj Niwas. GNCTD

27/C

रजिस्ट्री सं॰ डी॰ एल॰—(एन)04/0007/2003—23 REGISTERED NO. DL—(N)04/0007/2003—23

भारत का राजपत्र
The Gazette of India

सी.जी.-डी.एल.-अ.-12082023-248045
CG-DL-E-12082023-248045

असाधारण
EXTRAORDINARY
भाग II — खण्ड 1
PART II — Section 1
प्राधिकार से प्रकाशित
PUBLISHED BY AUTHORITY

सं॰ 25] नई दिल्ली, शुक्रवार, अगस्त 11, 2023/ श्रावण 20, 1945 (शक)
No. 25] NEW DELHI, FRIDAY, AUGUST 11, 2023/SRAVANA 20, 1945 (SAKA)

इस भाग में भिन्न पृष्ठ संख्या दी जाती है जिससे कि यह अलग संकलन के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW AND JUSTICE
(Legislative Department)

New Delhi, the 11*th August,* 2023/*Sravana* 20, 1945 (*Saka*)

The following Act of Parliament received the assent of the President on the 11th August, 2023 and is hereby published for general information:—

THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023
(No. 22 OF 2023)

[11*th August*, 2023.]

An Act to provide for the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventy-fourth Year of the Republic of India as follows:—

CHAPTER I
PRELIMINARY

Short title and commencement.

1. (*1*) This Act may be called the Digital Personal Data Protection Act, 2023.

(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Definitions.

2. In this Act, unless the context otherwise requires,—

(*a*) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997; 24 of 1997.

(*b*) "automated" means any digital process capable of operating automatically in response to instructions given or otherwise for the purpose of processing data;

(*c*) "Board" means the Data Protection Board of India established by the Central Government under section 18;

(*d*) "certain legitimate uses" means the uses referred to in section 7;

(*e*) "Chairperson" means the Chairperson of the Board;

(*f*) "child" means an individual who has not completed the age of eighteen years;

(*g*) "Consent Manager" means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform;

(*h*) "data" means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means;

(*i*) "Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data;

(*j*) "Data Principal" means the individual to whom the personal data relates and where such individual is—

(*i*) a child, includes the parents or lawful guardian of such a child;

(*ii*) a person with disability, includes her lawful guardian, acting on her behalf;

(*k*) "Data Processor" means any person who processes personal data on behalf of a Data Fiduciary;

(*l*) "Data Protection Officer" means an individual appointed by the Significant Data Fiduciary under clause (*a*) of sub-section (*2*) of section 10;

(*m*) "digital office" means an office that adopts an online mechanism wherein the proceedings, from receipt of intimation or complaint or reference or directions or appeal, as the case may be, to the disposal thereof, are conducted in online or digital mode;

(*n*) "digital personal data" means personal data in digital form;

(*o*) "gain" means—

(*i*) a gain in property or supply of services, whether temporary or permanent; or

(*ii*) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;

(*p*) "loss" means—

(*i*) a loss in property or interruption in supply of services, whether temporary or permanent; or

(*ii*) a loss of opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of legitimate remuneration;

(*q*) "Member" means a Member of the Board and includes the Chairperson;

(*r*) "notification" means a notification published in the Official Gazette and the expressions "notify" and "notified" shall be construed accordingly;

(*s*) "person" includes—

(*i*) an individual;

(*ii*) a Hindu undivided family;

(*iii*) a company;

(*iv*) a firm;

(*v*) an association of persons or a body of individuals, whether incorporated or not;

(*vi*) the State; and

(*vii*) every artificial juristic person, not falling within any of the preceding sub-clauses;

(*t*) "personal data" means any data about an individual who is identifiable by or in relation to such data;

(*u*) "personal data breach" means any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data;

(*v*) "prescribed" means prescribed by rules made under this Act;

(*w*) "proceeding" means any action taken by the Board under the provisions of this Act;

(*x*) "processing" in relation to personal data, means a wholly or partly automated operation or set of operations performed on digital personal data, and includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(*y*) "she" in relation to an individual includes the reference to such individual irrespective of gender;

(*z*) "Significant Data Fiduciary" means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10;

(*za*) "specified purpose" means the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder; and

(*zb*) "State" means the State as defined under article 12 of the Constitution.

Application of Act.

3. Subject to the provisions of this Act, it shall—

(*a*) apply to the processing of digital personal data within the territory of India where the personal data is collected—

(*i*) in digital form; or

(*ii*) in non-digital form and digitised subsequently;

(*b*) also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any activity related to offering of goods or services to Data Principals within the territory of India;

(*c*) not apply to—

(*i*) personal data processed by an individual for any personal or domestic purpose; and

(*ii*) personal data that is made or caused to be made publicly available by—

(*A*) the Data Principal to whom such personal data relates; or

(*B*) any other person who is under an obligation under any law for the time being in force in India to make such personal data publicly available.

Illustration.

X, an individual, while blogging her views, has publicly made available her personal data on social media. In such case, the provisions of this Act shall not apply.

CHAPTER II

OBLIGATIONS OF DATA FIDUCIARY

Grounds for processing personal data.

4. (*1*) A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and for a lawful purpose,—

(*a*) for which the Data Principal has given her consent; or

(*b*) for certain legitimate uses.

(*2*) For the purposes of this section, the expression "lawful purpose" means any purpose which is not expressly forbidden by law.

Notice.

5. (*1*) Every request made to a Data Principal under section 6 for consent shall be accompanied or preceded by a notice given by the Data Fiduciary to the Data Principal, informing her,—

(*i*) the personal data and the purpose for which the same is proposed to be processed;

(*ii*) the manner in which she may exercise her rights under sub-section (*4*) of section 6 and section 13; and

(*iii*) the manner in which the Data Principal may make a complaint to the Board,

in such manner and as may be prescribed.

Illustration.

X, an individual, opens a bank account using the mobile app or website of Y, a bank. To complete the Know-Your-Customer requirements under law for opening of bank account, X opts for processing of her personal data by Y in a live, video-based customer identification process. Y shall accompany or precede the request for the personal data with notice to X, describing the personal data and the purpose of its processing.

(*2*) Where a Data Principal has given her consent for the processing of her personal data before the date of commencement of this Act,—

(*a*) the Data Fiduciary shall, as soon as it is reasonably practicable, give to the Data Principal a notice informing her,—

(*i*) the personal data and the purpose for which the same has been processed;

(*ii*) the manner in which she may exercise her rights under sub-section (*4*) of section 6 and section 13; and

(*iii*) the manner in which the Data Principal may make a complaint to the Board,

in such manner and as may be prescribed.

(*b*) the Data Fiduciary may continue to process the personal data until and unless the Data Principal withdraws her consent.

Illustration.

X, an individual, gave her consent to the processing of her personal data for an online shopping app or website operated by Y, an e-commerce service provider, before the commencement of this Act. Upon commencement of the Act, Y shall, as soon as practicable, give through email, in-app notification or other effective method information to X, describing the personal data and the purpose of its processing.

(*3*) The Data Fiduciary shall give the Data Principal the option to access the contents of the notice referred to in sub-sections (*1*) and (*2*) in English or any language specified in the Eighth Schedule to the Constitution.

Consent.

6. (*1*) The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

Illustration.

X, an individual, downloads Y, a telemedicine app. Y requests the consent of X for (*i*) the processing of her personal data for making available telemedicine services, and (*ii*) accessing her mobile phone contact list, and X signifies her consent to both. Since phone contact list is not necessary for making available telemedicine services, her consent shall be limited to the processing of her personal data for making available telemedicine services.

(*2*) Any part of consent referred in sub-section (*1*) which constitutes an infringement of the provisions of this Act or the rules made thereunder or any other law for the time being in force shall be invalid to the extent of such infringement.

Illustration.

X, an individual, buys an insurance policy using the mobile app or website of Y, an insurer. She gives to Y her consent for (*i*) the processing of her personal data by Y for the purpose of issuing the policy, and (*ii*) waiving her right to file a complaint to the Data Protection Board of India. Part (*ii*) of the consent, relating to waiver of her right to file a complaint, shall be invalid.

(*3*) Every request for consent under the provisions of this Act or the rules made thereunder shall be presented to the Data Principal in a clear and plain language, giving her the option to access such request in English or any language specified in the Eighth Schedule to the Constitution and providing the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act.

(*4*) Where consent given by the Data Principal is the basis of processing of personal data, such Data Principal shall have the right to withdraw her consent at any time, with the ease of doing so being comparable to the ease with which such consent was given.

(*5*) The consequences of the withdrawal referred to in sub-section (*4*) shall be borne by the Data Principal, and such withdrawal shall not affect the legality of processing of the personal data based on consent before its withdrawal.

Illustration.

X, an individual, is the user of an online shopping app or website operated by Y, an e-commerce service provider. X consents to the processing of her personal data by Y for the purpose of fulfilling her supply order and places an order for supply of a good while making payment for the same. If X withdraws her consent, Y may stop enabling X to use the app or website for placing orders, but may not stop the processing for supply of the goods already ordered and paid for by X.

(*6*) If a Data Principal withdraws her consent to the processing of personal data under sub-section (*5*), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing the personal data of such Data Principal unless such processing without her consent is required or authorised under the provisions of this Act or the rules made thereunder or any other law for the time being in force in India.

Illustration.

X, a telecom service provider, enters into a contract with Y, a Data Processor, for emailing telephone bills to the customers of X. Z, a customer of X, who had earlier given her consent to X for the processing of her personal data for emailing of bills, downloads the mobile app of X and opts to receive bills only on the app. X shall itself cease, and shall cause Y to cease, the processing of the personal data of Z for emailing bills.

(*7*) The Data Principal may give, manage, review or withdraw her consent to the Data Fiduciary through a Consent Manager.

(*8*) The Consent Manager shall be accountable to the Data Principal and shall act on her behalf in such manner and subject to such obligations as may be prescribed.

(*9*) Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed.

(*10*) Where a consent given by the Data Principal is the basis of processing of personal data and a question arises in this regard in a proceeding, the Data Fiduciary shall be obliged to prove that a notice was given by her to the Data Principal and consent was given by such Data Principal to the Data Fiduciary in accordance with the provisions of this Act and the rules made thereunder.

Certain legitimate uses.

7. A Data Fiduciary may process personal data of a Data Principal for any of following uses, namely:—

(*a*) for the specified purpose for which the Data Principal has voluntarily provided her personal data to the Data Fiduciary, and in respect of which she has not indicated to the Data Fiduciary that she does not consent to the use of her personal data.

Illustrations.

(*I*) X, an individual, makes a purchase at Y, a pharmacy. She voluntarily provides Y her personal data and requests Y to acknowledge receipt of the payment made for the purchase by sending a message to her mobile phone. Y may process the personal data of X for the purpose of sending the receipt.

(*II*) X, an individual, electronically messages Y, a real estate broker, requesting Y to help identify a suitable rented accommodation for her and shares her personal data for this purpose. Y may process her personal data to identify and intimate to her the details of accommodation available on rent. Subsequently, X informs Y that X no longer needs help from Y. Y shall cease to process the personal data of X;

(*b*) for the State and any of its instrumentalities to provide or issue to the Data Principal such subsidy, benefit, service, certificate, licence or permit as may be prescribed, where—

(*i*) she has previously consented to the processing of her personal data by the State or any of its instrumentalities for any subsidy, benefit, service, certificate, licence or permit; or

(*ii*) such personal data is available in digital form in, or in non-digital form and digitised subsequently from, any database, register, book or other document which is maintained by the State or any of its instrumentalities and is notified by the Central Government,

subject to standards followed for processing being in accordance with the policy issued by the Central Government or any law for the time being in force for governance of personal data.

Illustration.

X. a pregnant woman, enrols herself on an app or website to avail of government's maternity benefits programme, while consenting to provide her personal data for the purpose of availing of such benefits. Government may process the personal data of X processing to determine her eligibility to receive any other prescribed benefit from the government;

(*c*) for the performance by the State or any of its instrumentalities of any function under any law for the time being in force in India or in the interest of sovereignty and integrity of India or security of the State;

(*d*) for fulfilling any obligation under any law for the time being in force in India on any person to disclose any information to the State or any of its instrumentalities, subject to such processing being in accordance with the provisions regarding disclosure of such information in any other law for the time being in force;

(*e*) for compliance with any judgment or decree or order issued under any law for the time being in force in India, or any judgment or order relating to claims of a contractual or civil nature under any law for the time being in force outside India;

(*f*) for responding to a medical emergency involving a threat to the life or immediate threat to the health of the Data Principal or any other individual;

(*g*) for taking measures to provide medical treatment or health services to any individual during an epidemic, outbreak of disease, or any other threat to public health;

(*h*) for taking measures to ensure safety of, or provide assistance or services to, any individual during any disaster, or any breakdown of public order.

Explanation.—For the purposes of this clause, the expression "disaster" shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster Management Act, 2005; or

53 of 2005.

(*i*) for the purposes of employment or those related to safeguarding the employer from loss or liability, such as prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information or provision of any service or benefit sought by a Data Principal who is an employee.

General obligations of Data Fiduciary.

8. (*1*) A Data Fiduciary shall, irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under this Act, be responsible for complying with the provisions of this Act and the rules made thereunder in respect of any processing undertaken by it or on its behalf by a Data Processor.

(*2*) A Data Fiduciary may engage, appoint, use or otherwise involve a Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals only under a valid contract.

(*3*) Where personal data processed by a Data Fiduciary is likely to be—

(*a*) used to make a decision that affects the Data Principal; or

(*b*) disclosed to another Data Fiduciary,

the Data Fiduciary processing such personal data shall ensure its completeness, accuracy and consistency.

(*4*) A Data Fiduciary shall implement appropriate technical and organisational measures to ensure effective observance of the provisions of this Act and the rules made thereunder.

(*5*) A Data Fiduciary shall protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a Data Processor, by taking reasonable security safeguards to prevent personal data breach.

(*6*) In the event of a personal data breach, the Data Fiduciary shall give the Board and each affected Data Principal, intimation of such breach in such form and manner as may be prescribed.

(*7*) A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force,—

(*a*) erase personal data, upon the Data Principal withdrawing her consent or as

soon as it is reasonable to assume that the specified purpose is no longer being served, whichever is earlier; and

(*b*) cause its Data Processor to erase any personal data that was made available by the Data Fiduciary for processing to such Data Processor.

Illustrations.

(*I*) X, an individual, registers herself on an online marketplace operated by Y, an e-commerce service provider. X gives her consent to Y for the processing of her personal data for selling her used car. The online marketplace helps conclude the sale. Y shall no longer retain her personal data.

(*II*) X, an individual, decides to close her savings account with Y, a bank. Y is required by law applicable to banks to maintain the record of the identity of its clients for a period of ten years beyond closing of accounts. Since retention is necessary for compliance with law, Y shall retain X's personal data for the said period.

(*8*) The purpose referred to in clause (*a*) of sub-section (*7*) shall be deemed to no longer be served, if the Data Principal does not—

(*a*) approach the Data Fiduciary for the performance of the specified purpose; and

(*b*) exercise any of her rights in relation to such processing,

for such time period as may be prescribed, and different time periods may be prescribed for different classes of Data Fiduciaries and for different purposes.

(*9*) A Data Fiduciary shall publish, in such manner as may be prescribed, the business contact information of a Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary, the questions, if any, raised by the Data Principal about the processing of her personal data.

(*10*) A Data Fiduciary shall establish an effective mechanism to redress the grievances of Data Principals.

(*11*) For the purposes of this section, it is hereby clarified that a Data Principal shall be considered as not having approached the Data Fiduciary for the performance of the specified purpose, in any period during which she has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.

Processing of personal data of children.

9. (*1*) The Data Fiduciary shall, before processing any personal data of a child or a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian, as the case may be, in such manner as may be prescribed.

Explanation.—For the purpose of this sub-section, the expression "consent of the parent" includes the consent of lawful guardian, wherever applicable.

(*2*) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause any detrimental effect on the well-being of a child.

(*3*) A Data Fiduciary shall not undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

(*4*) The provisions of sub-sections (*1*) and (*3*) shall not be applicable to processing of personal data of a child by such classes of Data Fiduciaries or for such purposes, and subject to such conditions, as may be prescribed.

(*5*) The Central Government may, if satisfied that a Data Fiduciary has ensured that its processing of personal data of children is done in a manner that is verifiably safe, notify for such processing by such Data Fiduciary the age above which that Data Fiduciary shall be exempt from the applicability of all or any of the obligations under sub-sections (*1*) and (*3*) in respect of processing by that Data Fiduciary as the notification may specify.

Additional obligations of Significant Data Fiduciary.

10. (*1*) The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of such relevant factors as it may determine, including—

(*a*) the volume and sensitivity of personal data processed;

(*b*) risk to the rights of Data Principal;

(*c*) potential impact on the sovereignty and integrity of India;

(*d*) risk to electoral democracy;

(*e*) security of the State; and

(*f*) public order.

(*2*) The Significant Data Fiduciary shall—

(*a*) appoint a Data Protection Officer who shall—

(*i*) represent the Significant Data Fiduciary under the provisions of this Act;

(*ii*) be based in India;

(*iii*) be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary; and

(*iv*) be the point of contact for the grievance redressal mechanism under the provisions of this Act;

(*b*) appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act; and

(*c*) undertake the following other measures, namely:—

(*i*) periodic Data Protection Impact Assessment, which shall be a process comprising a description of the rights of Data Principals and the purpose of processing of their personal data, assessment and management of the risk to the rights of the Data Principals, and such other matters regarding such process as may be prescribed;

(*ii*) periodic audit; and

(*iii*) such other measures, consistent with the provisions of this Act, as may be prescribed.

CHAPTER III

RIGHTS AND DUTIES OF DATA PRINCIPAL

Right to access information about personal data.

11. (*1*) The Data Principal shall have the right to obtain from the Data Fiduciary to whom she has previously given consent, including consent as referred to in clause (*a*) of section 7 (hereinafter referred to as the said Data Fiduciary), for processing of personal data, upon making to it a request in such manner as may be prescribed,—

(*a*) a summary of personal data which is being processed by such Data Fiduciary and the processing activities undertaken by that Data Fiduciary with respect to such personal data;

(*b*) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared by such Data Fiduciary, along with a description of the personal data so shared; and

(*c*) any other information related to the personal data of such Data Principal and its processing, as may be prescribed.

(*2*) Nothing contained in clause (*b*) or clause (*c*) of sub-section (*1*) shall apply in respect of the sharing of any personal data by the said Data Fiduciary with any other Data Fiduciary authorised by law to obtain such personal data, where such sharing is pursuant

to a request made in writing by such other Data Fiduciary for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

Right to correction and erasure of personal data.

12. (*1*) A Data Principal shall have the right to correction, completion, updating and erasure of her personal data for the processing of which she has previously given consent, including consent as referred to in clause (*a*) of section 7, in accordance with any requirement or procedure under any law for the time being in force.

(*2*) A Data Fiduciary shall, upon receiving a request for correction, completion or updating from a Data Principal,—

(*a*) correct the inaccurate or misleading personal data;

(*b*) complete the incomplete personal data; and

(*c*) update the personal data.

(*3*) A Data Principal shall make a request in such manner as may be prescribed to the Data Fiduciary for erasure of her personal data, and upon receipt of such a request, the Data Fiduciary shall erase her personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.

Right of grievance redressal.

13. (*1*) A Data Principal shall have the right to have readily available means of grievance redressal provided by a Data Fiduciary or Consent Manager in respect of any act or omission of such Data Fiduciary or Consent Manager regarding the performance of its obligations in relation to the personal data of such Data Principal or the exercise of her rights under the provisions of this Act and the rules made thereunder.

(*2*) The Data Fiduciary or Consent Manager shall respond to any grievances referred to in sub-section (*1*) within such period as may be prescribed from the date of its receipt for all or any class of Data Fiduciaries.

(*3*) The Data Principal shall exhaust the opportunity of redressing her grievance under this section before approaching the Board.

Right to nominate.

14. (*1*) A Data Principal shall have the right to nominate, in such manner as may be prescribed, any other individual, who shall, in the event of death or incapacity of the Data Principal, exercise the rights of the Data Principal in accordance with the provisions of this Act and the rules made thereunder.

(*2*) For the purposes of this section, the expression "incapacity" means inability to exercise the rights of the Data Principal under the provisions of this Act or the rules made thereunder due to unsoundness of mind or infirmity of body.

Duties of Data Principal.

15. A Data Principal shall perform the following duties, namely:—

(*a*) comply with the provisions of all applicable laws for the time being in force while exercising rights under the provisions of this Act;

(*b*) to ensure not to impersonate another person while providing her personal data for a specified purpose;

(*c*) to ensure not to suppress any material information while providing her personal data for any document, unique identifier, proof of identity or proof of address issued by the State or any of its instrumentalities;

(*d*) to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board; and

(*e*) to furnish only such information as is verifiably authentic, while exercising the right to correction or erasure under the provisions of this Act or the rules made thereunder.

CHAPTER IV

SPECIAL PROVISIONS

Processing of personal data outside India.

16. (*1*) The Central Government may, by notification, restrict the transfer of personal data by a Data Fiduciary for processing to such country or territory outside India as may be so notified.

(*2*) Nothing contained in this section shall restrict the applicability of any law for the time being in force in India that provides for a higher degree of protection for or restriction on transfer of personal data by a Data Fiduciary outside India in relation to any personal data or Data Fiduciary or class thereof.

Exemptions.

17. (*1*) The provisions of Chapter II, except sub-sections (*1*) and (*5*) of section 8, and those of Chapter III and section 16 shall not apply where—

(*a*) the processing of personal data is necessary for enforcing any legal right or claim;

(*b*) the processing of personal data by any court or tribunal or any other body in India which is entrusted by law with the performance of any judicial or quasi-judicial or regulatory or supervisory function, where such processing is necessary for the performance of such function;

(*c*) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law for the time being in force in India;

(*d*) personal data of Data Principals not within the territory of India is processed pursuant to any contract entered into with any person outside the territory of India by any person based in India;

(*e*) the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation of two or more companies or a reconstruction by way of demerger or otherwise of a company, or transfer of undertaking of one or more company to another company, or involving division of one or more companies, approved by a court or tribunal or other authority competent to do so by any law for the time being in force; and

(*f*) the processing is for the purpose of ascertaining the financial information and assets and liabilities of any person who has defaulted in payment due on account of a loan or advance taken from a financial institution, subject to such processing being in accordance with the provisions regarding disclosure of information or data in any other law for the time being in force.

Explanation.—For the purposes of this clause, the expressions "default" and "financial institution" shall have the meanings respectively assigned to them in sub-sections (*12*) and (*14*) of section 3 of the Insolvency and Bankruptcy Code, 2016.

31 of 2016.

Illustration.

X, an individual, takes a loan from Y, a bank. X defaults in paying her monthly loan repayment instalment on the date on which it falls due. Y may process the personal data of X for ascertaining her financial information and assets and liabilities.

(*2*) The provisions of this Act shall not apply in respect of the processing of personal data—

(*a*) by such instrumentality of the State as the Central Government may notify, in the interests of sovereignty and integrity of India, security of the State, friendly relations with foreign States, maintenance of public order or preventing incitement to any cognizable offence relating to any of these, and the processing by the Central Government of any personal data that such instrumentality may furnish to it; and

(*b*) necessary for research, archiving or statistical purposes if the personal data is not to be used to take any decision specific to a Data Principal and such processing is carried on in accordance with such standards as may be prescribed.

(*3*) The Central Government may, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries or class of Data Fiduciaries, including startups, as Data Fiduciaries to whom the provisions of section 5, sub-sections (*3*) and (*7*) of section 8 and sections 10 and 11 shall not apply.

Explanation.—For the purposes of this sub-section, the term "startup" means a private limited company or a partnership firm or a limited liability partnership incorporated in India, which is eligible to be and is recognised as such in accordance with the criteria and process notified by the department to which matters relating to startups are allocated in the Central Government.

(*4*) In respect of processing by the State or any instrumentality of the State, the provisions of sub-section (*7*) of section 8 and sub-section (*3*) of section 12 and, where such processing is for a purpose that does not include making of a decision that affects the Data Principal, sub-section (*2*) of section 12 shall not apply.

(*5*) The Central Government may, before expiry of five years from the date of commencement of this Act, by notification, declare that any provision of this Act shall not apply to such Data Fiduciary or classes of Data Fiduciaries for such period as may be specified in the notification.

CHAPTER V

DATA PROTECTION BOARD OF INDIA

Establishment of Board.

18. (*1*) With effect from such date as the Central Government may, by notification, appoint, there shall be established, for the purposes of this Act, a Board to be called the Data Protection Board of India.

(*2*) The Board shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

(*3*) The headquarters of the Board shall be at such place as the Central Government may notify.

Composition and qualifications for appointment of Chairperson and Members.

19. (*1*) The Board shall consist of a Chairperson and such number of other Members as the Central Government may notify.

(*2*) The Chairperson and other Members shall be appointed by the Central Government in such manner as may be prescribed.

(*3*) The Chairperson and other Members shall be a person of ability, integrity and standing who possesses special knowledge or practical experience in the fields of data governance, administration or implementation of laws related to social or consumer protection, dispute resolution, information and communication technology, digital economy, law, regulation or techno-regulation, or in any other field which in the opinion of the Central Government may be useful to the Board, and at least one among them shall be an expert in the field of law.

Salary, allowances payable to and term of office.

20. (*1*) The salary, allowances and other terms and conditions of service of the Chairperson and other Members shall be such as may be prescribed, and shall not be varied to their disadvantage after their appointment.

(*2*) The Chairperson and other Members shall hold office for a term of two years and shall be eligible for re-appointment.

Disqualifications for appointment and continuation as Chairperson and Members of Board.

21. (*1*) A person shall be disqualified for being appointed and continued as the Chairperson or a Member, if she—

(*a*) has been adjudged as an insolvent;

(*b*) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;

(*c*) has become physically or mentally incapable of acting as a Member;

(*d*) has acquired such financial or other interest, as is likely to affect prejudicially her functions as a Member; or

(*e*) has so abused her position as to render her continuance in office prejudicial to the public interest.

(*2*) The Chairperson or Member shall not be removed from her office by the Central Government unless she has been given an opportunity of being heard in the matter.

Resignation by Members and filling of vacancy.

22. (*1*) The Chairperson or any other Member may give notice in writing to the Central Government of resigning from her office, and such resignation shall be effective from the date on which the Central Government permits her to relinquish office, or upon expiry of a period of three months from the date of receipt of such notice, or upon a duly appointed successor entering upon her office, or upon the expiry of the term of her office, whichever is earliest.

(*2*) A vacancy caused by the resignation or removal or death of the Chairperson or any other Member, or otherwise, shall be filled by fresh appointment in accordance with the provisions of this Act.

(*3*) The Chairperson and any other Member shall not, for a period of one year from the date on which they cease to hold such office, except with the previous approval of the Central Government, accept any employment, and shall also disclose to the Central Government any subsequent acceptance of employment with any Data Fiduciary against whom proceedings were initiated by or before such Chairperson or other Member.

Proceedings of Board.

23. (*1*) The Board shall observe such procedure in regard to the holding of and transaction of business at its meetings, including by digital means, and authenticate its orders, directions and instruments in such manner as may be prescribed.

(*2*) No act or proceeding of the Board shall be invalid merely by reason of—

(*a*) any vacancy in or any defect in the constitution of the Board;

(*b*) any defect in the appointment of a person acting as the Chairperson or other Member of the Board; or

(*c*) any irregularity in the procedure of the Board, which does not affect the merits of the case.

(*3*) When the Chairperson is unable to discharge her functions owing to absence, illness or any other cause, the senior-most Member shall discharge the functions of the Chairperson until the date on which the Chairperson resumes her duties.

Officers and employees of Board.

24. The Board may, with previous approval of the Central Government, appoint such officers and employees as it may deem necessary for the efficient discharge of its functions under the provisions of this Act, on such terms and conditions of appointment and service as may be prescribed.

Members and officers to be public servants.

45 of 1860.

25. The Chairperson, Members, officers and employees of the Board shall be deemed, when acting or purporting to act in pursuance of provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code.

Powers of Chairperson.

26. The Chairperson shall exercise the following powers, namely:—

(*a*) general superintendence and giving direction in respect of all administrative matters of the Board;

(*b*) authorise any officer of the Board to scrutinise any intimation, complaint, reference or correspondence addressed to the Board; and

(*c*) authorise performance of any of the functions of the Board and conduct any of its proceedings, by an individual Member or groups of Members and to allocate proceedings among them.

CHAPTER VI

POWERS, FUNCTIONS AND PROCEDURE TO BE FOLLOWED BY BOARD

Powers and functions of Board.

27. (*1*) The Board shall exercise and perform the following powers and functions, namely:—

(*a*) on receipt of an intimation of personal data breach under sub-section (*6*) of section 8, to direct any urgent remedial or mitigation measures in the event of a personal data breach, and to inquire into such personal data breach and impose penalty as provided in this Act;

(*b*) on a complaint made by a Data Principal in respect of a personal data breach or a breach in observance by a Data Fiduciary of its obligations in relation to her personal data or the exercise of her rights under the provisions of this Act, or on a reference made to it by the Central Government or a State Government, or in compliance of the directions of any court, to inquire into such breach and impose penalty as provided in this Act;

(*c*) on a complaint made by a Data Principal in respect of a breach in observance by a Consent Manager of its obligations in relation to her personal data, to inquire into such breach and impose penalty as provided in this Act;

(*d*) on receipt of an intimation of breach of any condition of registration of a Consent Manager, to inquire into such breach and impose penalty as provided in this Act; and

(*e*) on a reference made by the Central Government in respect of the breach in observance of the provisions of sub-section (*2*) of section 37 by an intermediary, to inquire into such breach and impose penalty as provided in this Act.

(*2*) The Board may, for the effective discharge of its functions under the provisions of this Act, after giving the person concerned an opportunity of being heard and after recording reasons in writing, issue such directions as it may consider necessary to such person, who shall be bound to comply with the same.

(*3*) The Board may, on a representation made to it by a person affected by a direction issued under sub-section (*1*) or sub-section (*2*), or on a reference made by the Central Government, modify, suspend, withdraw or cancel such direction and, while doing so, impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

Procedure to be followed by Board.

28. (*1*) The Board shall function as an independent body and shall, as far as practicable, function as a digital office, with the receipt of complaints and the allocation, hearing and pronouncement of decisions in respect of the same being digital by design, and adopt such techno-legal measures as may be prescribed.

(*2*) The Board may, on receipt of an intimation or complaint or reference or directions as referred to in sub-section (*1*) of section 27, take action in accordance with the provisions of this Act and the rules made thereunder.

(*3*) The Board shall determine whether there are sufficient grounds to proceed with an inquiry.

(*4*) In case the Board determines that there are insufficient grounds, it may, for reasons to be recorded in writing, close the proceedings.

(*5*) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons to be recorded in writing, inquire into the affairs of any person for ascertaining whether such person is complying with or has complied with the provisions of this Act.

(*6*) The Board shall conduct such inquiry following the principles of natural justice and shall record reasons for its actions during the course of such inquiry.

(*7*) For the purposes of discharging its functions under this Act, the Board shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, in respect of matters relating to— 5 of 1908.

(*a*) summoning and enforcing the attendance of any person and examining her on oath;

(*b*) receiving evidence of affidavit requiring the discovery and production of documents;

(*c*) inspecting any data, book, document, register, books of account or any other document; and

(*d*) such other matters as may be prescribed.

(*8*) The Board or its officers shall not prevent access to any premises or take into custody any equipment or any item that may adversely affect the day-to-day functioning of a person.

(*9*) The Board may require the services of any police officer or any officer of the Central Government or a State Government to assist it for the purposes of this section and it shall be the duty of every such officer to comply with such requisition.

(*10*) During the course of the inquiry, if the Board considers it necessary, it may for reasons to be recorded in writing, issue interim orders after giving the person concerned an opportunity of being heard.

(*11*) On completion of the inquiry and after giving the person concerned an opportunity of being heard, the Board may for reasons to be recorded in writing, either close the proceedings or proceed in accordance with section 33.

(*12*) At any stage after receipt of a complaint, if the Board is of the opinion that the complaint is false or frivolous, it may issue a warning or impose costs on the complainant.

CHAPTER VII

APPEAL AND ALTERNATE DISPUTE RESOLUTION

29. (*1*) Any person aggrieved by an order or direction made by the Board under this Act may prefer an appeal before the Appellate Tribunal. Appeal to Appellate Tribunal.

(*2*) Every appeal under sub-section (*1*) shall be filed within a period of sixty days from the date of receipt of the order or direction appealed against and it shall be in such form and manner and shall be accompanied by such fee as may be prescribed.

(*3*) The Appellate Tribunal may entertain an appeal after the expiry of the period specified in sub-section (*2*), if it is satisfied that there was sufficient cause for not preferring the appeal within that period.

(*4*) On receipt of an appeal under sub-section (*1*), the Appellate Tribunal may, after giving the parties to the appeal, an opportunity of being heard, pass such orders thereon as it thinks fit, confirming, modifying or setting aside the order appealed against.

(5) The Appellate Tribunal shall send a copy of every order made by it to the Board and to the parties to the appeal.

(6) The appeal filed before the Appellate Tribunal under sub-section (1) shall be dealt with by it as expeditiously as possible and endeavour shall be made by it to dispose of the appeal finally within six months from the date on which the appeal is presented to it.

(7) Where any appeal under sub-section (6) could not be disposed of within the period of six months, the Appellate Tribunal shall record its reasons in writing for not disposing of the appeal within that period.

(8) Without prejudice to the provisions of section 14A and section 16 of the Telecom Regulatory Authority of India Act, 1997, the Appellate Tribunal shall deal with an appeal under this section in accordance with such procedure as may be prescribed. 24 of 1997.

(9) Where an appeal is filed against the orders of the Appellate Tribunal under this Act, the provisions of section 18 of the Telecom Regulatory Authority of India Act, 1997 shall apply. 24 of 1997.

(10) In respect of appeals filed under the provisions of this Act, the Appellate Tribunal shall, as far as practicable, function as a digital office, with the receipt of appeal, hearing and pronouncement of decisions in respect of the same being digital by design.

Orders passed by Appellate Tribunal to be executable as decree.

30. (1) An order passed by the Appellate Tribunal under this Act shall be executable by it as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

Alternate dispute resolution.

31. If the Board is of the opinion that any complaint may be resolved by mediation, it may direct the parties concerned to attempt resolution of the dispute through such mediation by such mediator as the parties may mutually agree upon, or as provided for under any law for the time being in force in India.

Voluntary undertaking.

32. (1) The Board may accept a voluntary undertaking in respect of any matter related to observance of the provisions of this Act from any person at any stage of a proceeding under section 28.

(2) The voluntary undertaking referred to in sub-section (1) may include an undertaking to take such action within such time as may be determined by the Board, or refrain from taking such action, and or publicising such undertaking.

(3) The Board may, after accepting the voluntary undertaking and with the consent of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking.

(4) The acceptance of the voluntary undertaking by the Board shall constitute a bar on proceedings under the provisions of this Act as regards the contents of the voluntary undertaking, except in cases covered by sub-section (5).

(5) Where a person fails to adhere to any term of the voluntary undertaking accepted by the Board, such breach shall be deemed to be breach of the provisions of this Act and the Board may, after giving such person an opportunity of being heard, proceed in accordance with the provisions of section 33.

CHAPTER VIII

PENALTIES AND ADJUDICATION

Penalties.

33. (1) If the Board determines on conclusion of an inquiry that breach of the provisions of this Act or the rules made thereunder by a person is significant, it may, after giving the

Consistency with other laws.

38. (*1*) The provisions of this Act shall be in addition to and not in derogation of any other law for the time being in force.

(*2*) In the event of any conflict between a provision of this Act and a provision of any other law for the time being in force, the provision of this Act shall prevail to the extent of such conflict.

Bar of jurisdiction.

39. No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power under the provisions of this Act.

Power to make rules.

40. (*1*) The Central Government may, by notification, and subject to the condition of previous publication, make rules not inconsistent with the provisions of this Act, to carry out the purposes of this Act.

(*2*) In particular and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:—

(*a*) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (*1*) of section 5;

(*b*) the manner in which the notice given by the Data Fiduciary to a Data Principal shall inform her, under sub-section (*2*) of section 5;

(*c*) the manner of accountability and the obligations of Consent Manager under sub-section (*8*) of section 6;

(*d*) the manner of registration of Consent Manager and the conditions relating thereto, under sub-section (*9*) of section 6;

(*e*) the subsidy, benefit, service, certificate, licence or permit for the provision or issuance of which, personal data may be processed under clause (*b*) of section 7;

(*f*) the form and manner of intimation of personal data breach to the Board under sub-section (*6*) of section 8;

(*g*) the time period for the specified purpose to be deemed as no longer being served, under sub-section (*8*) of section 8;

(*h*) the manner of publishing the business contact information of a Data Protection Officer under sub-section (*9*) of section 8;

(*i*) the manner of obtaining verifiable consent under sub-section (*1*) of section 9;

(*j*) the classes of Data Fiduciaries, the purposes of processing of personal data of a child and the conditions relating thereto, under sub-section (*4*) of section 9;

(*k*) the other matters comprising the process of Data Protection Impact Assessment under sub-clause (*i*) of clause (*c*) of sub-section (*2*) of section 10;

(*l*) the other measures that the Significant Data Fiduciary shall undertake under sub-clause (*iii*) of clause (*c*) of sub-section (*2*) of section 10;

(*m*) the manner in which a Data Principal shall make a request to the Data Fiduciary to obtain information and any other information related to the personal data of such Data Principal and its processing, under sub-section (*1*) of section 11;

(*n*) the manner in which a Data Principal shall make a request to the Data Fiduciary for erasure of her personal data under sub-section (*3*) of section 12;

(*o*) the period within which the Data Fiduciary shall respond to any grievances under sub-section (*2*) of section 13;

(*p*) the manner of nomination of any other individual by the Data Principal under sub-section (*1*) of section 14;

(*q*) the standards for processing the personal data for exemption under clause (*b*) of sub-section (*2*) of section 17;

(*r*) the manner of appointment of the Chairperson and other Members of the Board under sub-section (*2*) of section 19;

(*s*) the salary, allowances and other terms and conditions of services of the Chairperson and other Members of the Board under sub-section (*1*) of section 20;

(*t*) the manner of authentication of orders, directions and instruments under sub-section (*1*) of section 23;

(*u*) the terms and conditions of appointment and service of officers and employees of the Board under section 24;

(*v*) the techno-legal measures to be adopted by the Board under sub-section (*1*) of section 28;

(*w*) the other matters under clause (*d*) of sub-section (*7*) of section 28;

(*x*) the form, manner and fee for filing an appeal under sub-section (*2*) of section 29;

(*y*) the procedure for dealing an appeal under sub-section (*8*) of section 29;

(*z*) any other matter which is to be or may be prescribed or in respect of which provision is to be, or may be, made by rules.

Laying of rules and certain notifications.

41. Every rule made and every notification issued under section 16 and section 42 of this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or notification or both Houses agree that the rule or notification should not be made or issued, the rule or notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or notification.

Power to amend Schedule.

42. (*1*) The Central Government may, by notification, amend the Schedule, subject to the restriction that no such notification shall have the effect of increasing any penalty specified therein to more than twice of what was specified in it when this Act was originally enacted.

(*2*) Any amendment notified under sub-section (*1*) shall have effect as if enacted in this Act and shall come into force on the date of the notification.

Power to remove difficulties.

43. (*1*) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to it to be necessary or expedient for removing the difficulty.

(*2*) No order as referred to in sub-section (*1*) shall be made after the expiry of three years from the date of commencement of this Act.

(*3*) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

Amendments to certain Acts.

24 of 1997.

44. (*1*) In section 14 of the Telecom Regulatory Authority of India Act, 1997, in clause (*c*), for sub-clauses (*i*) and (*ii*), the following sub-clauses shall be substituted, namely:—

"(*i*) the Appellate Tribunal under the Information Technology Act, 2000; 21 of 2000.

(*ii*) the Appellate Tribunal under the Airports Economic Regulatory Authority of India Act, 2008; and 27 of 2008.

(*iii*) the Appellate Tribunal under the Digital Personal Data Protection Act, 2023.".

(*2*) The Information Technology Act, 2000 shall be amended in the following manner, namely:— 21 of 2000.

(*a*) section 43A shall be omitted;

(*b*) in section 81, in the proviso, after the words and figures "the Patents Act, 1970", the words and figures "or the Digital Personal Data Protection Act, 2023" shall be inserted; and 39 of 1970.

(*c*) in section 87, in sub-section (*2*), clause (*ob*) shall be omitted.

(*3*) In section 8 of the Right to Information Act, 2005, in sub-section (*1*), for clause (*j*), the following clause shall be substituted, namely:— 22 of 2005.

"(*j*) information which relates to personal information;".

THE SCHEDULE

[*See* section 33 (*1*)]

Sl. No.	Breach of provisions of this Act or rules made thereunder	Penalty
(1)	(2)	(3)
1.	Breach in observing the obligation of Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (*5*) of section 8.	May extend to two hundred and fifty crore rupees.
2.	Breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach under sub-section (*6*) of section 8.	May extend to two hundred crore rupees.
3.	Breach in observance of additional obligations in relation to children under section 9.	May extend to two hundred crore rupees.
4.	Breach in observance of additional obligations of Significant Data Fiduciary under section 10.	May extend to one hundred and fifty crore rupees.
5.	Breach in observance of the duties under section 15.	May extend to ten thousand rupees.
6.	Breach of any term of voluntary undertaking accepted by the Board under section 32.	Up to the extent applicable for the breach in respect of which the proceedings under section 28 were instituted.
7.	Breach of any other provision of this Act or the rules made thereunder.	May extend to fifty crore rupees.

DR. REETA VASISHTA,
Secretary to the Govt. of India.

UPLOADED BY THE MANAGER, GOVERNMENT OF INDIA PRESS, MINTO ROAD, NEW DELHI–110002
AND PUBLISHED BY THE CONTROLLER OF PUBLICATIONS, DELHI–110054.

MGIPMRND—288GI—11-08-2023.

16\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

71

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

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

15/C

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>

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 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) 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

Ministry of Electronics and Information Technology
Government of India

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;*

- *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.

82

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.

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.

****

84