The Ministry of Electronics and Information Technology invites feedback on the draft 'Digital Personal Data Protection Bill, 2022'.

Ministry of Electronics and Information Technology has been deliberating on various aspects of digital personal data and its protection, and has formulated a draft Bill, titled 'The Digital Personal Data Protection Bill, 2022'. The purpose of the draft Bill is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.

The draft Bill employs plain and simple language to facilitate ease of understanding and is available on Ministry's website at https://www.meity.gov.in/data-protection-framework, along with an Explanatory note that provides a brief overview of its provisions, which is available at https://www.meity.gov.in/data-protection-framework

The Digital Personal Data Protection Bill frames out the rights and duties of the citizen (Digital Nagrik) on one hand and the obligations to use collected data lawfully of the Data Fiduciary on the other hand. The bill is based on the following principles around the Data Economy:

The Bill will establish the comprehensive legal framework governing digital personal data protection in India. The Bill provides for the processing of digital personal data in a manner that recognizes the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes.

The Ministry has invited feedback from the public on the draft Bill. The submissions will not be disclosed and held in fiduciary capacity, to enable persons submitting feedback to provide the same freely. No public disclosure of the submissions will be made.

The feedback on the draft bill in a chapter wise manner may be submitted on MyGov website (Link will be provided shortly) by 17th December 2022.

***

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

THE DIGITAL PERSONAL DATA PROTECTION BILL, 2022

The purpose of this Act is to provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes, and for matters connected therewith or incidental thereto.

Chapter 1: PRELIMINARY

1. Short Title and Commencement

(1) This Act may be called the Digital Personal Data Protection Act, 2022.

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

2. Definitions

In this Act:–

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

(2) “Board” means the Data Protection Board of India established by the Central Government for the purposes of this Act;

(3) “child” means an individual who has not completed eighteen years of age;

(4) “data” means a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means;

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

(6) “Data Principal” means the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child;

(7) “Data Processor” means any person who processes personal data on behalf of a Data Fiduciary;

(8) “Data Protection Officer” means an individual appointed as such by a Significant Data Fiduciary under the provisions of this Act;

(9) “gain” means-

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

(b) an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

(10) “harm”, in relation to a Data Principal, means -

a. any bodily harm; or
b. distortion or theft of identity; or
c. harassment; or
d. prevention of lawful gain or causation of significant loss;

(11) “loss” means –

a. a loss in property or interruption in supply of services, whether temporary or permanent; or

b. a loss of an opportunity to earn remuneration or greater remuneration or to gain a financial advantage otherwise than by way of remuneration.

(12) “person” includes—

(a) an individual;

(b) a Hindu Undivided Family;

(c) a company;

(d) a firm;

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

(f) the State; and

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

(13) “personal data” means any data about an individual who is identifiable by or in relation to such data;

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

(15) “prescribed” means prescribed by Rules made under the provisions of this Act;

(16) “processing” in relation to personal data means an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(17) “proceeding” means any action taken by the Board under the provisions of this Act;

(18) “public interest” means in the interest of any of the following:

(a) sovereignty and integrity of India;

b. security of the State;
c. friendly relations with foreign States;
d. maintenance of public order;
e. preventing incitement to the commission of any cognizable offence relating to the preceding sub-clauses; and
f. preventing dissemination of false statements of fact.

3. Interpretation

In this Act: -

(1) unless the context otherwise requires, a reference to “*provisions of this Act*” shall be read as including a reference to Rules made under this Act.

(2) “*the option to access … in English or any language specified in the Eighth Schedule to the Constitution of India*” shall mean that the Data Principal may select either English or any one of the languages specified in the Eighth Schedule to the Constitution of India;

(3) the pronouns “her” and “she” have been used for an individual, irrespective of gender.

4. Application of the Act

(1) The provisions of this Act shall apply to the processing of digital personal data within the territory of India where:

(a) such personal data is collected from Data Principals online; and

(b) such personal data collected offline, is digitized.

(2) The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India.

For the purpose of this sub-section, “profiling” means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal.

(3) The provisions of this Act shall not apply to:

(a) non-automated processing of personal data;

(b) offline personal data;

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

(d) personal data about an individual that is contained in a record that has been in existence for at least 100 years.

Chapter 2: OBLIGATIONS OF DATA FIDUCIARY

5. Grounds for processing digital personal data

A person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act.

For the purpose of this Act, “lawful purpose” means any purpose which is not expressly forbidden by law.

6. Notice

(1) On or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of processing of such personal data.

(2) Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable.

For the purpose of this section: -

(a) “notice” can be a separate document, or an electronic form, or a part of the same document in or through which personal data is sought to be collected, or in such other form as may be prescribed.

(b) “itemised” means presented as a list of individual items.

Illustration*: ‘A’ contacts a bank to open a regular savings account. The bank asks ‘A’ to furnish photocopies of proof of address and identity for KYC formalities. Before collecting the photocopies, the bank should give notice to ‘A’ stating that the purpose of obtaining the photocopies is completion of KYC formalities. The notice need not be a separate document. It can be printed on the form used for opening the savings bank account.*

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

7. Consent

(1) Consent of the Data Principal means any freely given, specific, informed and unambiguous indication of the Data Principal's wishes by which the Data Principal, by a clear affirmative action, signifies agreement to the processing of her personal data for the specified purpose.

For the purpose of this sub-section, “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.

(2) Any part of consent referred in sub-section (1) which constitutes an infringement of provisions of this Act shall be invalid to the extent of such infringement.

Illustration*: ‘A’ enters into a contract with ‘B’ to provide a service ‘X’ to ‘B’. As part of the contract, ‘B’ consents to: (a) processing of her personal data by ‘A’, and (b) waive her right to file a complaint with the Board under the provisions of this Act. Part (b) of the consent by which ‘B’ has agreed to waive her right shall be considered invalid.*

(3) Every request for consent under the provisions of this Act shall be presented to the Data Principal in a clear and plain language, along with 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. The Data Fiduciary shall give to the Data Principal the

option to access such request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.

(4) Where consent given by the Data Principal is the basis of processing of personal data, the Data Principal shall have the right to withdraw her consent at any time. The consequences of such withdrawal shall be borne by such Data Principal. The withdrawal of consent shall not affect the lawfulness of processing of the personal data based on consent before its withdrawal. The ease of such withdrawal shall be comparable to the ease with which consent may be given.

***Illustration**: 'A' enters into a contract with 'B' to provide a service 'X' to 'B'. As part of the contract, 'B' consents to processing of her personal data by 'A'. If 'B' withdraws her consent to processing of her personal data, 'A' may stop offering the service 'X' to 'B'.*

(5) If a Data Principal withdraws her consent to the processing of personal data under sub-section (4), the Data Fiduciary shall, within a reasonable time, cease and cause its Data Processors to cease processing of the personal data of such Data Principal unless such processing without the Data Principal's consent is required or authorised under the provisions of this Act or any other law.

***Illustration**: 'A' subscribes to an e-mail and SMS-based sales notification service operated by 'B'. As part of the subscription contract, 'A' shares her personal data including mobile number and e-mail ID with 'B' which shares it further with 'C', a Data Processor for the purpose of sending alerts to 'A' via e-mail and SMS. If 'A' withdraws her consent to processing of her personal data, 'B' shall stop and cause 'C' to stop processing the personal data of 'A'.*

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

For the purpose of this section, a "Consent Manager" is a Data Fiduciary which enables a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

(7) The Consent Manager specified in this section shall be an entity that is accountable to the Data Principal and acts on behalf of the Data Principal. 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.

(8) The performance of any contract already concluded between a Data Fiduciary and a Data Principal shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.

Illustration*: If 'A' enters into a contract with 'B' to provide a service 'X' to 'B' then 'A' shall not deny to provide service 'X' to 'B' on B's refusal to give consent for collection of additional personal data which is not necessary for the purpose of providing service 'X'.*

(9) Where 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 the Data Fiduciary to the Data Principal and consent was given by the Data Principal to the Data Fiduciary in accordance with the provisions of this Act.

8. Deemed consent

A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary:

(1) in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data;

Illustration*: 'A' shares her name and mobile number with a Data Fiduciary for the purpose of reserving a table at a restaurant. 'A' shall be deemed to have given her consent to the collection of her name and mobile number by the Data Fiduciary for the purpose of confirming the reservation.*

(2) for the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State;

Illustration*: 'A' shares her name, mobile number and bank account number with a government department for direct credit of agricultural income support. 'A' shall be deemed to have given her consent to the processing of her name, mobile number and bank account number for the purpose of credit of fertilizer subsidy amount to her bank account.*

(3) for compliance with any judgment or order issued under any law;

(4) 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;

(5) 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;

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

(7) for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance;

Illustration*: 'A' shares her biometric data with her employer 'B' for the purpose of marking A's attendance in the biometric attendance system installed at A's workplace. 'A' shall be deemed to have given her consent to the processing of her biometric data for the purpose of verification of her attendance.*

(8) in public interest, including for:

(a) prevention and detection of fraud;

(b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws;

(c) network and information security;

(d) credit scoring;

(e) operation of search engines for processing of publicly available personal data;

(f) processing of publicly available personal data; and

(g) recovery of debt;

(9) for any fair and reasonable purpose as may be prescribed after taking into consideration:

a. whether the legitimate interests of the Data Fiduciary in processing for that purpose outweigh any adverse effect on the rights of the Data Principal;
b. any public interest in processing for that purpose; and
c. the reasonable expectations of the Data Principal having regard to the context of the processing.

9. General obligations of Data Fiduciary

(1) A Data Fiduciary shall, irrespective of any agreement to the contrary, or non-compliance of a Data Principal with her duties specified in this Act, be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf by a Data Processor or another Data Fiduciary.

(2) A Data Fiduciary shall make reasonable efforts to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete, if the personal data:

(a) is likely to be used by the Data Fiduciary to make a decision that affects the Data Principal to whom the personal data relates; or

(b) is likely to be disclosed by the Data Fiduciary to another Data Fiduciary.

***Illustration**: 'A' has instructed her mobile service provider 'B' to mail physical copies of monthly bills to her postal address. Upon a change in her postal address, 'A' duly informs 'B' of her new postal address and completes necessary KYC formalities. 'B' should ensure that the postal address of 'A' is updated accurately in its records.*

(3) A Data Fiduciary shall implement appropriate technical and organizational measures to ensure effective adherence with the provisions of this Act.

(4) Every Data Fiduciary and Data Processor shall protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breach.

(5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed.

For the purpose of this section “affected Data Principal” means any Data Principal to whom any personal data affected by a personal data breach relates.

(6) A Data Fiduciary must cease to retain personal data, or remove the means by which the personal data can be associated with particular Data Principals, as soon as it is reasonable to assume that:

(a) the purpose for which such personal data was collected is no longer being served by its retention; and

(b) retention is no longer necessary for legal or business purposes.

Illustration (A)*: ‘A’ creates an account on ‘X’, a Social Media Platform. As part of the process of creating the account, ‘A’ shares her personal data with ‘X’. After three months, ‘A’ deletes the account. Once ‘A’ deletes the account, ‘X’ must stop retaining the personal data of ‘A’ or remove the means by which the personal data of ‘A’ can be associated with ‘A’.*

Illustration (B)*: ‘A’ opens a savings account with a bank. As part of KYC formalities, ‘A’ shares her personal data with the bank. After six months, ‘A’ closes the savings account with the bank. As per KYC rules, the bank is required to retain personal data for a period beyond six months. In this case, the bank may retain ‘A’s’ personal data for the period prescribed in KYC Rules because such retention is necessary for a legal purpose.*

(7) Every 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 Data Principal’s questions about the processing of her personal data.

(8) Every Data Fiduciary shall have in place a procedure and effective mechanism to redress the grievances of Data Principals.

(9) The Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data on its behalf, only under a valid contract. Such Data Processor may, if permitted under its contract with the Data Fiduciary, further engage, appoint, use, or involve another Data Processor in processing personal data only under a valid contract.

10. Additional obligations in relation to processing of personal data of children

(1) The Data Fiduciary shall, before processing any personal data of a child, obtain verifiable parental consent in such manner as may be prescribed.

For the purpose of this section, “parental consent” includes the consent of lawful guardian, where applicable.

(2) A Data Fiduciary shall not undertake such processing of personal data that is likely to cause harm to a child, as may be prescribed.

(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 for such purposes, as may be prescribed.

11. Additional obligations of Significant Data Fiduciary

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 relevant factors, including:

a. the volume and sensitivity of personal data processed;
b. risk of harm to the Data Principal;
c. potential impact on the sovereignty and integrity of India;
d. risk to electoral democracy;
e. security of the State;
f. public order; and
g. such other factors as it may consider necessary;

(2) The Significant Data Fiduciary shall:

(a) appoint a Data Protection Officer who shall represent the Significant Data Fiduciary under the provisions of this Act and be based in India. The Data Protection Officer shall be an individual responsible to the Board of Directors or similar governing body of the Significant Data Fiduciary. The Data Protection officer shall be the point of contact for the grievance redressal mechanism under the provisions of this Act;

(b) appoint an Independent Data Auditor who shall evaluate the compliance of the Significant Data Fiduciary with provisions of this Act; and

(c) undertake such other measures including Data Protection Impact Assessment and periodic audit in relation to the objectives of this Act, as may be prescribed.

For the purpose of this section, “Data Protection Impact Assessment” means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed.

Chapter 3: RIGHTS & DUTIES OF DATA PRINCIPAL

12. Right to information about personal data

The Data Principal shall have the right to obtain from the Data Fiduciary:

(1) the confirmation whether the Data Fiduciary is processing or has processed personal data of the Data Principal;

(2) a summary of the personal data of the Data Principal being processed or that has been processed by the Data Fiduciary and the processing activities undertaken by the Data Fiduciary with respect to the personal data of the Data Principal;

(3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared; and

(4) any other information as may be prescribed.

13. Right to correction and erasure of personal data

(1) A Data Principal shall have the right to correction and erasure of her personal data, in accordance with the applicable laws and in such manner as may be prescribed.

(2) A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal:

(a) correct a Data Principal’s inaccurate or misleading personal data;

(b) complete a Data Principal’s incomplete personal data;

(c) update a Data Principal’s personal data;

(d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.

14. Right of grievance redressal

(1) A Data Principal shall have the right to readily available means of registering a grievance with a Data Fiduciary.

(2) A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed, may register a complaint with the Board in such manner as may be prescribed.

15. Right to nominate.

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.

For the purpose of this section, “incapacity” means inability to exercise the rights of the Data Principal under the provisions of this Act due to unsoundness of mind or body.

16. Duties of Data Principal.

(1) A Data Principal shall comply with the provisions of all applicable laws while exercising rights under the provisions of this Act.

(2) A Data Principal shall not register a false or frivolous grievance or complaint with a Data Fiduciary or the Board.

(3) A Data Principal shall, under no circumstances including while applying for any document, service, unique identifier, proof of identity or proof of address, furnish any false particulars or suppress any material information or impersonate another person.

(4) A Data Principal shall furnish only such information as is verifiably authentic while exercising the right to correction or erasure under the provisions of this Act.

Chapter 4: SPECIAL PROVISIONS

17. Transfer of personal data outside India

The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.

18. Exemptions.

(1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act 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 is necessary for the performance of any judicial or quasi-judicial function;

(c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law;

(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.

(2) The Central Government may, by notification, exempt from the application of provisions of this Act, the processing of personal data:

a. by any instrumentality of the State 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

(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 standards specified by the Board.

(3) The Central Government may by notification, having regard to the volume and nature of personal data processed, notify certain Data Fiduciaries

or class of Data Fiduciaries as Data Fiduciary to whom the provisions of Section 6, sub-sections (2) and (6) of section 9, sections 10, 11 and 12 of this Act shall not apply.

(4) The provisions of sub-section (6) of section 9 of this Act shall not apply in respect of processing by the State or any instrumentality of the State.

Chapter 5: COMPLIANCE FRAMEWORK

19. Data Protection Board of India

(1) The Central Government shall, by notification, establish, for the purposes of this Act, a Board to be called the Data Protection Board of India. The allocation of work, receipt of complaints, formation of groups for hearing, pronouncement of decisions, and other functions of the Board shall be digital by design.

(2) The strength and composition of the Board and the process of selection, terms and conditions of appointment and service, removal of its Chairperson and other Members shall be such as may be prescribed.

(3) The chief executive entrusted with the management of the affairs of the Board shall be such individual as the Central Government may appoint and terms and conditions of her service shall be such as the Central Government may determine.

(4) The Board shall have such other officers and employees, with such terms and conditions of appointment and service, as may be prescribed.

(5) 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.

(6) No suit, prosecution or other legal proceedings shall lie against the Board or its Chairperson, Member, employee or officer for anything which is done or intended to be done in good faith under the provisions of this Act.

20. Functions of the Board

(1) The functions of the Board are:

(a) to determine non-compliance with provisions of this Act and impose penalty under the provisions of this Act; and

(b) to perform such functions as the Central Government may assign to the Board under the provisions of this Act or under any other law by an order published in the Official Gazette.

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

(3) The Board may, in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.

(4) The Board may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (2) and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

21. Process to be followed by the Board to ensure compliance with the provisions of the Act

(1) The Board shall function as an independent body and, as far as possible, function as a digital office and employ such techno-legal measures as may be prescribed.

(2) The Board may, on receipt of a complaint made by an affected person or on a reference made to it by the Central Government or a State Government or in compliance with the directions of any court or in case of non-compliance with section 16 of this Act by a Data Principal, take action in accordance with the provisions of this Act.

(3) The Board may authorise conduct of proceedings relating to complaints, by individual Members or groups of Members.

(4) The Board shall first determine whether there are sufficient grounds to proceed with an inquiry. In case the Board determines that there are insufficient grounds, it may, for reasons recorded in writing, close such proceeding.

(5) In case the Board determines that there are sufficient grounds to proceed with inquiry, it may, for reasons 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 including giving reasonable opportunity of being heard and shall record reasons for its actions during the course of such inquiry.

(7) For the purpose of conduct of inquiry under this section, the Board shall have powers to summon and enforce the attendance of persons, examine them on oath and inspect any data, book, document, register, books of account or any other document.

(8) Inquiry under this section shall be completed at the earliest. 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 for preventing non-compliance with the provisions of this Act, it may, for reasons to be recorded in writing, issue interim orders after giving the concerned persons a reasonable opportunity of being heard.

(11) On conclusion of the inquiry and after giving the concerned persons a reasonable opportunity of being heard, if the Board determines that non-compliance by a person is not significant, it may, for reasons recorded in writing, close such inquiry. If the Board determines that the non-compliance by the person is significant, it shall proceed in accordance with section 25 of this Act.

(12) At any stage after receipt of a complaint, if the Board determines that the complaint is devoid of merit, it may issue a warning or impose costs on the complainant.

(13) Every person shall be bound by the orders of the Board. Every order made by the Board shall be enforced by it as if it were a decree made by a Civil Court. For the purpose of this sub-section, the Board shall have all the powers of a Civil Court as provided in the Code of Civil Procedure, 1908.

22. Review and Appeal

(1) The Board may review its order, acting through a group for hearing larger than the group which held proceedings in a matter under section 21, on a representation made to it, or on its own, and for reasons to be recorded in writing, modify, suspend, withdraw or cancel any order issued under the provisions of this Act and in doing so, may impose such conditions as it may deem fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

(2) An appeal against any order of the Board shall lie to the High Court. Every appeal made under this section shall be preferred within a period of sixty days from the date of the order appealed against.

(3) No civil court shall have the jurisdiction to entertain any suit or take any action in respect of any matter under the provisions of this Act and no injunction shall be granted by any court or other authority in respect of any action taken under the provisions of this Act.

23. Alternate Dispute Resolution

If the Board is of the opinion that any complaint may more appropriately be resolved by mediation or other process of dispute resolution, the Board may direct the concerned parties to attempt resolution of the dispute through mediation by a body or group of persons designated by the Board or such other process as the Board may consider fit.

24. Voluntary Undertaking

(1) The Board may accept a voluntary undertaking in respect of any matter related to compliance with provisions of this Act from any person at any stage.

(2) Such voluntary undertaking may include an undertaking to take specified action within a specified time, an undertaking to refrain from taking specified action, and an undertaking to publicize the voluntary undertaking.

(3) The Board may, after accepting the voluntary undertaking and with the agreement of the person who gave the voluntary undertaking vary the terms included in the voluntary undertaking. 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 (4).

(4) Where a person fails to comply with any term of the voluntary undertaking accepted by the Board, the Board may, after giving such person,

a reasonable opportunity of being heard, proceed in accordance with section 25 of this Act.

25. Financial Penalty

(1) If the Board determines on conclusion of an inquiry that non-compliance by a person is significant, it may, after giving the person a reasonable opportunity of being heard, impose such financial penalty as specified in Schedule 1, not exceeding rupees five hundred crore in each instance.

(2) While determining the amount of a financial penalty to be imposed under sub-section (1), the Board shall have regard to the following matters:

(a) the nature, gravity and duration of the non-compliance;

(b) the type and nature of the personal data affected by the non-compliance;

(c) repetitive nature of the non-compliance;

(d) whether the person, as a result of the non-compliance, has realized a gain or avoided any loss;

(e) whether the person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action;

(f) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the provisions of this Act; and

(g) the likely impact of the imposition of the financial penalty on the person.

Chapter 6: MISCELLANEOUS

26. Power to make Rules

(1) The Central Government may, by, notification make Rules consistent with the provisions of this Act to carry out the provisions of this Act.

(2) Every Rule made under the provisions of this Act shall be laid as soon as may be after it is made, before each House of the 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 both Houses agree that the rule should not be made, the rule 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.

27. Power of Central Government to amend Schedules

(1) The Central Government may, by notification, amend Schedule 1 to this Act. No such notification shall have the effect of increasing a penalty specified in Schedule 1 to more than double of what was specified in Schedule 1 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, unless the notification otherwise directs.

(3) Every amendment made by the Central Government under sub-section (1) shall be laid as soon as may be after it is made, before each House of the 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 amendment or both Houses agree that the amendment should not be made, the amendment 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 amendment.

28. Removal of difficulties

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, before expiry of five years from the date of commencement of this Act, by an 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) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

29. Consistency with other laws

1. The provisions of this Act shall be in addition to, and not construed in derogation of the provisions of any other law, and shall be construed as consistent with such 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.

30. Amendments.

(1) The Information Technology Act, 2000 ("IT Act") shall be amended in the following manner:

(a) section 43A of the IT Act shall be omitted;

(b) In section 81 of the IT Act, in the proviso, after the words and figures "the Patents Act, 1970", the words "or the Digital Personal Data Protection Act, 2022" shall be inserted; and

(c) clause (ob) of sub-section (2) of section 87 of IT Act shall be omitted.

(2) Clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 shall be amended in the following manner:

(a) The words "the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information" shall be omitted;

b. The proviso shall be omitted.

Schedule 1

(See section 25)

Sl. No.	Subject matter of the non-compliance	Penalty
(1)	**(2)**	**(3)**
1	Failure of Data Processor or Data Fiduciary to take reasonable security safeguards to prevent personal data breach under sub-section (4) of section 9 of this Act	Penalty up to Rs 250 crore
2	Failure to notify the Board and affected Data Principals in the event of a personal data breach, under sub-section (5) of section 9 of this Act	Penalty up to Rs 200 crore
3	Non-fulfilment of additional obligations in relation to Children; under section 10 of this Act	
4	Non-fulfilment of additional obligations of Significant Data Fiduciary; under section 11 of this Act	Penalty up to Rs 150 crore
5	Non-compliance with section 16 of this Act	Penalty up to Rs 10 thousand
6	Non-compliance with provisions of this Act other than those listed in (1) to (5) and any Rule made thereunder	Penalty up to Rs 50 crore