KNOWLEDGE BANK™

Always stay curious

MCO LEGALS

26th September, 2023

CYBER LAW: ISSUE 14

JOURNEY FROM THE BILL TO AN ACT: HIGHLIGHTS OF THEKEY CHANGES IN THE DIGITAL PERSONAL DATA PROTECTION ACT 2023

Amit Meharia

Managing Partner, MCO Legals

LLB (Hons) King's College London, Solicitor (Supreme Court of England & Wales)

Expertise:

Corporate Due Diligence & Corporate/Commercial Arbitration

amit.m@mcolegals.co.in

India has recently introduced its first-ever Privacy law, called the Digital Personal Data Protection Act, 2023' ("Act"). The legislation has successfully been approved from all the channels and received President's assent on 11th August 2023. Subsequently, it was officially announced in the official gazette. The primary objective of this Act is to regulate the handling of digital personal data, balancing the rights of individuals to safeguard their personal information with the necessity of processing such data for lawful purposes. The 21-page document, the Act is remarkably comprehensive yet concise, encompassing all significant rights and obligations essential for safeguarding an individual's digital personal data along with fixing accountability and penalties in case of data breaches and non-compliances. Previously MCO Legal Knowledge Bank published an overview of the Digital Data Protection Bill 2022. In this piece, we aim to highlight the changes in the Bill that are eventually approved and inculcated in the Act now.

Introduction	**Change in the Digital Personal Data Protection Act 2023**
Inclusion of New Definitions	• The Act now provides a definition of 'Appellate Tribunal' which will hear appeals arising from the Act. [S. 2(a)] • The Act has included the definition of 'Certain Legitimate Use Case'. [S. 2(d)] • Definition of 'digital office' is provided which 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. [S.2(m)] • The Act provides a definition of 'digital personal data'. It defines 'digital personal data' as personal data in digital form. The whole Act revolves around the protection of digital personal data and to justify the essence of the title of the Act completely, it was eminent to provide for the definition of 'digital personal data'. [S.2(n)] • The term 'specific purpose' is added defining as 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 there under.[S.2(za)]
Applicability of the Act	• The Act applies to the processing of digital personal data within the territory of India where the personal data is collected in digital form. The Act also extends its scope to the processing of digital personal data outside India, if such processing is in connection with any activity related to offering goods or services to Data Principles within India. Previously the word 'profiling' was used in place of 'activity' in Section 3(b) of the Act, and the removal of

Bhavna Sharma

Research Partner

B.Sc., LLM, Research Scholar, RML National Law University, Lucknow

	the term 'profiling' and its meaning thereby, shows the intent of the government to cover any sort of activity related to the processing of digital personal data and not only restrict it to 'profiling'. The term 'activity' now may include not only profiling but also, data analytics, behavioural, financial, and other tracking, user engagement analysis, personalization, and segmentation, etc. Though, the Act doesn't take in its ambit the data processed for personal or domestic purposes or any publicly available data or data made public under any legal obligation. [S. 3]
Grounds for Processing of digital personal data	• One of the additional grounds for the processing of digital personal data is added along with consent and i.e. 'for certain legitimate uses'. Now the Processing of personal data is permissible by the Data Fiduciary only with the consent of the Data Principal or for legitimate purposes. Here, the processing of personal data is allowed only for lawful purposes, that is, any purpose not expressly forbidden by law. The rightful way of taking consent is by way of a notice. The notice must contain any information regarding the personal data being collected and the purpose behind the processing of such personal data. It should also include the manner in which the Data Principal can exercise her rights and can make a complaint to the Data Protection Board and the contact details of the data protection officer or concerned person responsible for responding to Data Principal's request. [(S. 5 and S.4)] • This term 'legitimate use' is a replacement for the concept of 'deemed consent' that was previously there in the bill. A list of certain legitimate uses is provided under section 7 of the Act; the wording of the provision has been narrowed down now. The Act states that if the Data Principal voluntarily provides a Data Fiduciary with her personal data and requests Data Fiduciary for a particular service, it is deemed that the Data Principal has provided consent for the "specified purposes" and did not restrict the Data Fiduciaries from processing it for that purpose.
Consent Mechanism	• The word 'unconditional' is a new condition added to section 6(1) that talks about the essentials of consent. As per the amended section, the consent given by the Data Principal shall be informed, unconditional, and unambiguous with clear affirmative action, and shall signify an agreement to the processing of the personal data for the specific purpose and be limited to such personal data. The notice should be clear and in plain language and provided in English or any language specified in the 8th Schedule of the Indian Constitution. Under the Act, the Data Principal has a right to withdraw consent at any time. [S. 6]. • The Act now provides that the consent managers 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. [S.6(8)].
Modified General Obligations of Data Fiduciary	• Under section 8 of the Act, clause (2) has been inserted that allows Data Fiduciary to engage, appoint, use, or otherwise involve a Data Processor to process personal data only for specified purposes only under a valid contract. The Act also restricts the Data Processor to further involve another Data processor for the processing of digital personal data. • In the Bill, there was a shared responsibility of both Data Fiduciary and Data Processor in taking reasonable security safeguards to prevent personal data breaches. Now in the Act, it is only the responsibility of the Data Fiduciary alone to protect personal data in its possession or under its control or processing taken on its behalf to prevent a personal data breach. [S.8(5)]. • In the Bill, both Data Fiduciary and Data Processor were responsible for notifying the data breach to the Data Protection Board and the Data Principle. Now in the Act, it is only the Data Fiduciary to do so. [S.8(6)] • An additional ground 'withdrawal of consent' is added to Section 8(7)(b) of the Act that obliges the Data Fiduciary to delete the personal data of the Data Principal along with deleting personal data when the purpose of the collection is achieved, and the further retention is no longer necessary for any legal compliance requirement.

Rights of the Data Principal	• An exemption has been added to the right to access information where the Data Fiduciary can deny sharing the information about the identity of the other Data Fiduciary or Data Processor with whom the personal data has been shared requested the sharing of such information for the purpose of prevention, or detection, or investigation of offences or cyber incidents or prosecution or punishment of offences. [S.11(2)] • In addition to the right to correction and erasure of personal data, the Act now clearly states that this right also includes the right to completion and updation of personal data. [S.12(1)]. • The right of grievance redressal is now extendable not only to the Data Fiduciary but also to the Consent Managers. [S.13]
Cross Border Data Flows	• Under the Act, cross-border data transfer is allowed to any geographical jurisdiction outside India unless it is found that such jurisdiction prevents the applicability of this Act, and thereby the government black list such jurisdiction and restricts the data flows to such jurisdiction. Before the government thought of assessing the geographical jurisdictions on certain terms and conditions and subsequently notify the list of jurisdictions where the cross border data transfer may be allowed. [S.16]
Exemptions	• In addition to exemptions provided to courts or tribunals or any other body which performs any judicial or quasi-judiciary function from certain provisions of the Act, now the exemption is extended to regulators and supervisory authorities as well. [S.17(1)(b)] • The Act also provides exemptions where the processing is necessary for a scheme of compromise or arrangement or merger or amalgamation, or reconstruction by way of demerger, or transfer of undertaking of one or more companies to another, or involving division of one or more, approved by a court or tribunal or other authority competent to do so by law for the time being in force. [S.17(1)(e)] • Another exemption is provided for processing loans or in default of payment purposes. [S.17(1)(f)]
Data Protection Board	• Before the Act didn't mention anything about terms and conditions for appointment and services of the chairperson and other members of the Board. Now the Act provides clear requirements that the chairperson and members must possess to be a part of the Board. [S.19] • New sections are added regarding disqualification for appointment and continuation as Chairperson and members of the Board and Resignation by members and filling the vacancy. [S.21 & 22]
Appeals to TDSAT(Telecom Dispute Settlement Appellate Tribunal)	• Before there was no provision regarding the appellate tribunal, now the Act designates TDSAT as the appellate tribunal to hear the appeals arising against the order or direction of the Board.

What is there to look ahead?

The drafting of this Act by the Indian Government follows a principle-based approach that is most suitable and well-aligned with India's needs, requirements, and the potential impact of such regulations on the country's overall growth. Given that India is relatively new to the realm of privacy regulations, it's worth noting that initially, entities designated as "Data Fiduciary" according to the Act's definition might perceive the compliance burden as substantial and demanding. Nevertheless, it's the right time for India to come up with a Privacy law, considering the nation's rapid expansion in the digital sphere and the potential risk associated with the misuse of personal data belonging to Indian citizens. Several challenges exist in the successful implementation of this Act. These include gaps in the interpretation and understanding of the Act as the Rules to be made under various provisions are still underway, digital illiteracy among the populace, lack of privacy rights awareness, and lack of privacy experts. The Act does not stipulate a specific grace period for compliance, though generally, it takes around 6 – 12 months for a law to get implemented. Consequently, there's a significant likelihood that the Act will be introduced gradually, adopting a phased and incremental approach.

In spite of the challenges, it's important to remain optimistic about the potential of the Act. Its introduction signifies a crucial step in safeguarding the privacy rights of Indian citizens and addressing the intricacies of the digital age.

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

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

(*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.

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.

45 of 1860.

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

Appeal to Appellate Tribunal.

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.

(*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

person an opportunity of being heard, impose such monetary penalty specified in the Schedule.

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

(*a*) the nature, gravity and duration of the breach;

(*b*) the type and nature of the personal data affected by the breach;

(*c*) repetitive nature of the breach;

(*d*) whether the person, as a result of the breach, has realised a gain or avoided any loss;

(*e*) whether the person took any action to mitigate the effects and consequences of the breach, and the timeliness and effectiveness of such action;

(*f*) whether the monetary penalty to be imposed is proportionate and effective, having regard to the need to secure observance of and deter breach of the provisions of this Act; and

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

Crediting sums realised by way of penalties to Consolidated Fund of India.

34. All sums realised by way of penalties imposed by the Board under this Act, shall be credited to the Consolidated Fund of India.

CHAPTER IX

MISCELLANEOUS

Protection of action taken in good faith.

35. No suit, prosecution or other legal proceedings shall lie against the Central Government, the Board, its Chairperson and any Member, officer or employee thereof for anything which is done or intended to be done in good faith under the provisions of this Act or the rules made thereunder.

Power to call for information.

36. The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as it may call for.

Power of Central Government to issue directions.

37. (*1*) The Central Government or any of its officers specially authorised by it in this behalf may, upon receipt of a reference in writing from the Board that—

(*a*) intimates the imposition of monetary penalty by the Board on a Data Fiduciary in two or more instances; and

(*b*) advises, in the interests of the general public, the blocking for access by the public to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to Data Principals within the territory of India,

after giving an opportunity of being heard to that Data Fiduciary, on being satisfied that it is necessary or expedient so to do, in the interests of the general public, for reasons to be recorded in writing, by order, direct any agency of the Central Government or any intermediary to block for access by the public or cause to be blocked for access by the public any such information.

(*2*) Every intermediary who receives a direction issued under sub-section (*1*) shall be bound to comply with the same.

(*3*) For the purposes of this section, the expressions "computer resource", "information" and "intermediary" shall have the meanings respectively assigned to them in the Information Technology Act, 2000. 21 of 2000.

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, 21 of 2000. namely:—

(*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" 39 of 1970. shall be inserted; and

(*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*), 22 of 2005. the following clause shall be substituted, namely:—

"(*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.

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) 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) 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