DEEPSTRAT

STRATEGY . POLICY . ACTION

Analysis of the Digital Personal Data Protection Bill, 2023

Shachi Solanki

About DeepStrat

DeepStrat is a think tank and strategic consultancy registered as a section 2 entity under India's Companies Act 2013. It combines the rich experience and expertise of its founders and strategic advisers in government and the private sector. Among its founders, three are from the Indian Police Service (IPS), two from the Indian Foreign Service (IFS), and one each from the military, cybersecurity and risk management.

DeepStrat and its partner organisations bring its network and experience in multiple sectors:

Public Policy, Tax advisory, Cybersecurity, Technology, Project Design & Implementation, Risk Assessment & Management, Security, Foreign Policy.

It has published research on a wide range of issues, while delivering customised and sustainable solutions for its clients on a range of issues ranging from policy, cybersecurity, taxation, risk management and technology solutions.

About the Author

Shachi Solanki is the Deputy Chief of Operations at DeepStrat. She has studied Law from National Law University, Delhi (NLUD).

DPDP Bill, 2023	DPDP Bill, 2022	Comparison	Analysis
2(a) "Appellate Tribunal" means the Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997		Added "Appellate Tribunal" in the definitions section.	S. 2(a) read with S. 29 provides for filing of appeal with the Telecom Disputes Settlement and Appellate Tribunal, in contrast with the earlier provision of first appeal with the High Court.
2(f) Child "child" means an individual who has not completed the age of eighteen years;	**2(3). Child** "child" means an individual who has not completed eighteen years of age	-	
(g) Consent Manager "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	**7(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.	Consent manager has now been defined in the definition section.	
2(j). Data Principal "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; and (ii) a person with disability, includes their lawful guardian, acting on her behalf;	**2(6). Data Principal** "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	Removed – *"a person with disability, includes their lawful guardian, acting on behalf of such individual"*	- The Data Principal has a right under S. 15 to nominate another individual, who can exercise her rights in the event of her death or incapacity. This person need not be her lawful guardian. - Incapacity includes unsoundness of mind or infirmity of body.

(m) Digital Office "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;	-	Inserted a definition of digital office	Lends more clarity on the functioning of the Board.
2(n). Digital Personal Data Means personal data in digital form.	-	Inserted a new definition.	- Helps clarify the scope of the Act.
-	**2(10). Harm** "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	- Removed the definition of harm. - Added an Explanation to S. 10 which defines harm in relation to a child as – *"harm" means any detrimental effect on the well-being of a child.*	- The criteria for determining detrimental effect has not been laid down.
2(x). Processing "processing" in relation to personal data means a wholly or partly 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	**2(16). Processing** "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	Inserted – *"wholly or partly"*	Processing is not restricted only to automated processing, but now also includes processing with part-human intervention.
(za) Specified purpose "specified purpose" means the purpose mentioned in the notice given by	-	Definition of specified purpose has been inserted.	Lends clarity that data can only be processed for purposes

the Data Fiduciary to the Data Principal in accordance with the provisions of this Act and the rules made thereunder;			mentioned in the notice, on the basis of which the data principal has given her consent.
-	**2(18). Public interest** "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.	Removed the definition of public interest.	The contours of "public interest" have not been laid down.
3. Application of the Act (1) The provisions of this Act shall apply to processing – (a) within the territory of India of – (i) personal data collected in digital form; and (ii) personal data collected in non-digital form and digitised subsequently; and (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.	**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		- Removed the earlier grounds for non-applicability of the Act. New grounds where the Act does not apply have been added. Two instances where the Act will not apply are – 1. personal data processed by an individual for any personal or domestic purpose and 2. Personal data that is made or caused to be made publicly available. - If the processing of data is done outside India, that will also

(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.	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.		be covered if it is in connection with any activity related to offering of goods or services to Data Principals within the territory of India. But not if it is in connection with profiling alone.
6. Consent (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.	**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.	Inserted *"unconditional"* and *"with a clear affirmative action"* Inserted – *"and be limited to such personal data as is necessary for the specified purpose."*	- The consent has to be unconditional and indicated through a clear affirmative action. - A purpose limitation clause has been added. This additional safeguard will be useful for restricting disproportionate processing of personal data. - Consent will form the basis of processing data and it can only be done for the specified purpose mentioned in the notice "and" be limited to only such data as is

			necessary for the specified purpose. This language now reflects the principles of purpose limitation and necessity.
7. Certain legitimate uses 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. (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	**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; (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; (3) for compliance with any judgment or order issued under any law; (7) for the purposes related to employment, including prevention of corporate espionage, maintenance of	- -Added Sub-section 8.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."* - Added Sub-section 8.b.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 "* - Added – Sub – Section (8.b.ii)*"subject to standards followed for processing being in accordance with the policy issued by the Central Government or any*	- This section provides for processing of digital personal data without consent, earlier referred to as "deemed consent". - The data fiduciary can process data when the data principal has given consent, for a specified purpose, if she has not indicated that she does not consent to its processing. - Replaced the criteria of reasonable expectation with express denial of consent. - Personal data can be processed without consent also for issuing subsidy, benefit, service, certificate, license or permit. This can be done by the State or any of its instrumentalities. This provision is quite broad – it allows the State to use personal data which was previously given consent for use for *any other* subsidy, benefit, etc. It also

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.	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 (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	*law for the time being in force for governance of personal data."* - Removed *"(1) It is reasonably expected that she would provide such personal data"* - Removed *"verification of attendance and assessment of performance"* - Removed "public interest" as a ground for deemed consent. - Removed the "fair and reasonable purpose" clause - Removed *"Sub-section (7), (9)*	allows the State to use any personal data that is digitised from any database, register, book or any other document of the State. This will allow processing of personal data for government schemes for which the principal has not given consent. - The public interest clause which left the provision open to wide interpretation, has been removed. - The removal of "fair and reasonable purpose" clause has circumscribed the scope of the section to an extent.

	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.		
8. General obligations of data fiduciary (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	**9. General obligations of data fiduciary** (1) A Data Fiduciary shall, irrespective of any agreement to the contrary, or noncompliance 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. (3) A Data Fiduciary shall implement appropriate technical and organizational measures to ensure effective adherence	- Removed Section 9(1) *"processing undertaken by it or on behalf by a data processor or another Data Fiduciary"* -Added Sub-section 8(2) " Removed "*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."* - Added Subsection (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*	- Data fiduciary has to ensure that personal data is complete, accurate and consistent. - Data will be erased upon the Data Principal withdrawing her consent, as well as when the purpose limitation kicks in. - Purpose limitation for erasure of data kicks in when – 1. The data principal does not approach the data fiduciary for the performance of specified purpose or 2. She does not exercise her rights for such processing for a time as may be prescribed.

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	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.	*Prescribed."* - Removed – Sub-section (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."* -Removed Sub-section (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:"* -Added Sub-Section(7) *"A Data Fiduciary shall, unless retention is necessary for compliance with any law for the time being in force:"* - Added a ground for erasure of

Fiduciary for processing to such Data Processor. (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	personal data in sub-section (7)(a) “ - Added *Sub-section (8)-(11)*

has not initiated contact with the Data Fiduciary for such performance, in person or by way of communication in electronic or physical form.			
9. Processing of personal data of children (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	**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.	-Added a new sub-section 9(5) -Added Sub-section9(1) " *a person with disability who has a lawful guardian obtain verifiable consent of the parent of such child or the lawful guardian"* - Removed sub-section 10(2) *"likely to cause harm to a child, as may be prescribed"* -Changed the language in sub-section (2) from *"likely to cause harm to a child, as may be prescribed"* to *"likely to cause any detrimental effect on the well-being of a child"*	- Such processing which is likely to cause detrimental effect on the well-being of a child is not allowed. It is not clear what "detrimental effect on the well-being of a child" means. - The Central Government has the power to exempt certain Data Fiduciaries from complying with any or all provisions of this section, for children above a specified age, if it is ensured that the processing of their data is done in a verifiably safe manner.

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.			
10. 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 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;	**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;	- Removed "(*g) such other factors as it may consider necessary*" - Changed the language sub-section 10(1)(b) to *"risk to the rights of Data Principal"* from the earlier *"risk of harm to Data Principal".* -Added Sub-section 10 (2)(c)(i), (ii) & (iii)	- The classification of significant data fiduciary will now be on the basis of a defined criteria. - They will be classified as significant on the basis also of risk to the rights of Data Principal. Earlier the criterion read risk of harm to the Data Principal. - Removed the open-ended

(d) risk to electoral democracy; (e) security of the State; (f) public order.	(d) risk to electoral democracy; (e) security of the State; (f) public order; and (g) such other factors as it may consider necessary;		criterion of other factors as the Central Government may consider necessary.
11. Right to access information about personal data (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	**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.	-Added right to access personal information about data collected on the basis of certain legitimate uses under S. 7(a). -Added sub-section 11(2)	- Data that has been collected for legitimate use cases without consent under S. 7(a) will also be eligible for Data Principal's right to information about its processing. - In rest of the legitimate use cases, there will be no right to access information about one's personal data. - The right to receive the identities of entities with whom data has been shared will also not be available in cases where it has been shared for the purpose of prevention or detection or investigation of offences or cyber incidents, or for prosecution or punishment of offences.

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.			
12. Right to correction and erasure of personal data (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;	**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	- Inserted sub-section (3) – " *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.*"	- Data Principal has been given the right to get her personal data completed and updated. - This right extends also to data collected on the basis of deemed consent. - Right to erasure will not exist if retention is necessary for specified purpose or for compliance with law.

(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.	processed unless retention is necessary for a legal purpose.		
13. Right of grievance redressal (1) A Data Principal shall have the right to 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 grievances referred to in sub-section (1) within such period as may be prescribed from the date of its receipt for	**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.	- Added *"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."*	- Data fiduciaries and consent managers need to have a readily available means of grievance redressal. - The timeline of responding to grievances within a period of seven days has been removed. - It has been clarified that the Data Principal can only approach the Board after exhausting the grievance redressal mechanism available with the Data Fiduciary or

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.			Consent Manager.
15. Duties of Data Principal. 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.	**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.	Added sub-section 1(b) – " *to ensure not to impersonate another person while providing her personal data for a specified purpose;"* -Added sub-section (d) *"to ensure not to register a false or frivolous grievance or complaint with a Data Fiduciary or the Board;"*	Added a new duty of data principal – shall not impersonate another person.

16. Processing of personal data outside India (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.	**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.	- The language of sub-section 1 has changed *to "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."* - Added sub-section (2).	- Shift from the whitelisting approach, to allowing free cross-border flow of data to any territory, unless it is blacklisted. - If any other Indian law provides a higher threshold for protection or restricts cross-border transfer of data, that law will prevail.
17. Exemptions (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;	**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	- Inserted " *(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*	- "Any other body in India which is entrusted by law…" can in exercise of its "regulatory or supervisory function" also process personal data. This is a new addition and expands the scope of the section to new bodies. - Exemption from adhering to the law is also given in cases of companies where they reach a scheme for compromise, arrangement, merger or amalgamation, restructuring transfer, or division.

(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.	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,	*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. "* - Added *"The Central Government may, before expiry of five years from the date of commencement of this Act, declare by notification 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."*	- Exemption from processing of personal data, including financial data is also given in cases of investigation in loan default cases. - The Central Government's power to exempt "any instrumentality of the State" has been limited to "such instrumentality of the State" as has been notified (as opposed to *any* instrumentality). This change may limit the scope of exemption to some extent. - It has been clarified that start-ups may be excluded from cpmplying with certain provisions of this Act. - The Central Government can further exempt data fiduciaries from the applicability of this Act through a notification till 5 years from the enactment of this Act.

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

(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

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.

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.

18. Establishment of Board (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.	**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.	- Added *"The Board shall be a body corporate…"* -	- Made Board a Body Corporate.

	(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.		
19. Composition and qualifications for appointment of Chairperson and Members. (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		Added structure and strength of the Board – Sub-section (1),(2) & (3)	Prescribed the structure and strength of the Board. It will be headed by a Chairperson and other members, as prescribed. - Established a broad qualification criteria for selection of Board members. - Mandated one member to be a legal expert. - However, the appointment remains at the Central government's discretion.

an expert in the field of law.			
20. Salary, allowances payable to and the term of office			- The term of office of members will be 2 years, with provision for re-appointment.
20. Disqualifications for appointment and continuation as Chairperson and Members of Board. (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.	-	- Inserted grounds for disqualification.	

22. Resignation by Members and filling of vacancy. (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.	-	- Inserted provision on resignation of members - Inserted provision on filling of vacancy - Inserted terms for subsequent employment of Board members. - Added safeguard against employment with a Data Fiduciary that the Board conducted proceedings against.	

23. Proceedings of Board. (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.	-	Inserted a new section.	The manner of proceedings of the Board will be prescribed at a later stage through rules.
24. Officers and employees of Board. 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	-	Inserted a new section.	

and conditions of appointment and service as may be prescribed.			
25. Members and officers to be public servants 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.	-	Inserted a new section.	
26. Powers of Chairperson. 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.	-	Inserted a new section.	- The Chairperson will carry the functions of general superintendence of administrative matters, allocation of proceedings and will conduct proceedings.
27. Powers and functions of the Board(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	-	Added Section 27.	- The powers and functions of the Board, which earlier were left undefined have been elaborated in this Section.

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 36 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.			
28. Procedure to be followed by Board. (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.	-	-	- The Board can will function as a digital office, in that all the proceedings will be online. - It will have to follow the principles of natural justice while conducting an inquiry. - The Board shall have the powers of civil court for

(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— (a) summoning and enforcing the attendance			the purposes of conducting its proceedings.

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.			
29. Appeal to Appellate Tribunal. (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.	**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.	-	- Aggrieved persons may file an appeal before the TDSAT. - Appeal shall be tried to be disposed of by the TDSAT within a period of six months from the date of its presentation. - Section 18 of the Telecom Regulatory Authority of India Act, 1997 provides that appeals from orders of TDSAT can be filed before the Supreme Court within a period of 90 days. - The Appellate Tribunal will function as a digital office for the purposes of appeals under this Bill.

(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.

(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.

(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.			
30. Orders passed by Appellate Tribunal to be executable as decree. (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.	-	- Added a new section on orders of the Appellate Tribunal.	-
31. Alternate dispute resolution. 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	**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	- Removed *"Or other process of dispute resolution"* - Changed the process of appointment of mediator – *"such mediator as the parties may mutually agree upon, or as provided for under any law*	- The scope of ADR has been limited to mediation. - The mediator will be appointed either through mutual agreement of partier or in accordance with the Arbitration and Conciliation Act, 1996.

for the time being in force in India.	group of persons designated by the Board or such other process as the Board may consider fit.	- *for the time being in force in India"*	
32. Voluntary Undertaking (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	**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.	- Inserted *"at any stage of a proceeding under section 28."* The rest of the sub-sections remain the same in meaning.	- Explained the scope of this provision. Voluntary undertaking may only be given during the proceeding, not after its completion.

and the Board may, after giving such person an opportunity of being heard, proceed in accordance with the provisions of section 33.			
33. Penalties (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	**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.	- Removed *"not exceeding rupees five hundred crore in each instance"* - Added Sub-section (1)&(2*)*	- Reduction in maximum financial penalty from INR 500 crore (5 billion) to INR 250 crore (2.5 billion).

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.			
35. Protection of action taken in good faith 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.	**19(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.	Added *"Central Government"* to the list.	- Central government has been exempted from liability for acts done in "good faith". This provision may be overbroad and prone to misuse in the absence of safeguards.
36. Power to call for information The Central Government may, for the purposes of this Act, require the Board and any Data Fiduciary or intermediary to furnish such information as the Central Government may call for.	-	Inserted new section.	- Gives wide power to the Central Government without any provision for safeguards.
40. Power to make Rules (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		- Added the aspects that will be dealt with through Rules. - Subsection 2(a) will be dealt with under sub-section (2) of section 5 - Sub-section 2(b) will be dealt with under sub-section (2) of section 5	- A lot of nuances remain to be prescribed through Rules.

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		- Sub-section 2(c) will be dealt with under sub-section (8) of section 6 - Sub-section 2(d) will be dealt with under sub-section (9) of section 6 - Sub-section 2(e) will be dealt with under clause(b) of section 7 - Sub-section 2(f) will be dealt with under sub-section (6) of section 8 - Sub-section 2(g) will be dealt with under sub-section (8) of section 8 - Sub-section 2(h) will be dealt with under sub-section (9) of section 8 - Sub-section 2(i); manner of receiving verifiable consent as per sub-section (1) of section 9 - Sub-section 2(j) will be dealt with under sub-section (4) of section 9 - Sub-section 2(k) will be dealt with under sub-clause (i) of clause (c) of sub-section (2) of section 10;	

(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;		- Sub-section 2(l) will be dealt with under sub-clause (iii) of clause (c) of sub-section (2) of section 10 - Sub-section 2(m) will be dealt with under sub-section (1) of section 11 - Sub-section 2(n) will be dealt with under sub-section (3) of section 12 - Sub-section 2(o) will be dealt with under sub-section (2) of section 13.	
44. Amendments. (2) The Information Technology Act, 2000 shall be amended in the following manner, namely:— (a) section 43A shall be omitted;	**30. Amendments**. (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	Retained the amendment to the RTI Act.	- The scope of the RTI Act has been diluted which will affect citizens’ rights to seek information from public officials.

(b) in section 81, in the proviso, after the words and figures *"the Patents Act, 1970",* the words and figures "or *the Digital Personal Data Protection Act, 2023"* shall be inserted; and (c) in section 87, in sub-section (2), clause (ob) shall be omitted. (3) In section 8 of the Right to Information Act, 2005, in sub-section (1), for clause (j), the following clause shall be substituted, namely:— "(j) information which relates to personal information;"	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.		- The proviso that is sought to be omitted in the RTI Act applies to the whole of Section 8(1), and not just to S. 8(1)(j). This means that *any* information that cannot be denied to the Parliament or the State legislature cannot be denied to any person. The consequence of this amendment will be an erosion of the RTI, wherein citizens will not be able to seek information from public officials even if it pertained to public activity or if they are answerable for the same to the Parliament.

DEEPSTRAT

STRATEGY . POLICY . ACTION

www.deepstrat.in